ISC SSCP : Practice Test

Exam Code: SSCP

Title : System Security Certified Practitioner

Exam A

QUESTION 1
A potential problem related to the physical installation of the Iris Scanner in regards to the usage of the iris pattern within a biometric system is:

A. concern that the laser beam may cause eye damage
B. the iris pattern changes as a person grows older.
C. there is a relatively high rate of false accepts.
D. the optical unit must be positioned so that the sun does not shine into the aperture.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Because the optical unit utilizes a camera and infrared light to create the images, sun light can impact the aperture so it must not be positioned in direct light of any type. Because the subject does not need to have direct contact with the optical reader, direct light can impact the reader.
An Iris recognition is a form of biometrics that is based on the uniqueness of a subject's iris. A camera like device records the patterns of the iris creating what is known as Iriscode. It is the unique patterns of the iris that allow it to be one of the most accurate forms of biometric identification of an individual. Unlike other types of biometics, the iris rarely changes over time. Fingerprints can change over time due to scaring and manual labor, voice patterns can change due to a variety of causes, hand geometry can also change as well. But barring surgery or an accident it is not usual for an iris to change. The subject has a high-resoulution image taken of their iris and this is then converted to Iriscode. The current standard for the Iriscode was developed by John Daugman. When the subject attempts to be authenticated an infrared light is used to capture the iris image and this image is then compared to the Iriscode. If there is a match the subject's identity is confirmed. The subject does not need to have direct contact with the optical reader so it is a less invasive means of authentication then retinal scanning would be.
Reference(s) used for this question:
AIO, 3rd edition, Access Control, p 134.
AIO, 4th edition, Access Control, p 182.
Wikipedia - http://en.wikipedia.org/wiki/Iris_recognition The following answers are incorrect:
concern that the laser beam may cause eye damage. The optical readers do not use laser so, concern that the laser beam may cause eye damage is not an issue. the iris pattern changes as a person grows older. The question asked about the physical installation of the scanner, so this was not the best answer. If the question would have been about long term problems then it could have been the best choice. Recent research has shown that Irises actually do change over time: http://www.nature.com/news/ageing-eyes-hinder-biometric-scans-1.10722
there is a relatively high rate of false accepts. Since the advent of the Iriscode there is a very low rate of false accepts, in fact the algorithm used has never had a false match. This all depends on the quality of the equipment used but because of the uniqueness of the iris even when comparing identical twins, iris patterns are unique.

QUESTION 2
In Mandatory Access Control, sensitivity labels attached to object contain what information?

A. The item's classification
B. The item's classification and category set
C. The item's category
D. The items's need to know

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: A Sensitivity label must contain at least one classification and one category set. Category set and

Compartment set are synonyms, they mean the same thing. The sensitivity label must contain at least one Classification and at least one Category. It is common in some environments for a single item to belong to multiple categories. The list of all the categories to which an item belongs is called a compartment set or category set.
The following answers are incorrect:
the item's classification. Is incorrect because you need a category set as well. the item's category. Is incorrect because category set and classification would be both be required.
The item's need to know. Is incorrect because there is no such thing. The need to know is indicated by the catergories the object belongs to. This is NOT the best answer.
Reference(s) used for this question:
OIG CBK, Access Control (pages 186 - 188)
AIO, 3rd Edition, Access Control (pages 162 - 163)
AIO, 4th Edittion, Access Control, pp 212-214.
Wikipedia - http://en.wikipedia.org/wiki/Mandatory_Access_Control

QUESTION 3
What are the components of an object's sensitivity label?

A. A Classification Set and a single Compartment.

B. A single classification and a single compartment.

C. A Classification Set and user credentials.

D. A single classification and a Compartment Set.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Both are the components of a sensitivity label.
The following are incorrect:
A Classification Set and a single Compartment. Is incorrect because the nomenclature "Classification Set" is incorrect, there only one classifcation and it is not a "single compartment" but a Compartment Set.
A single classification and a single compartment. Is incorrect because while there only is one classifcation, it is not a "single compartment" but a Compartment Set. A Classification Set and user credentials. Is incorrect because the nomenclature "Classification Set" is incorrect, there only one classifcation and it is not "user credential" but a Compartment Set.
The user would have their own sensitivity label.

QUESTION 4
What does it mean to say that sensitivity labels are "incomparable"?

A. The number of classification in the two labels is different.

B. Neither label contains all the classifications of the other.

C. the number of categories in the two labels are different.

D. Neither label contains all the categories of the other.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: If a category does not exist then you cannot compare it. Incomparable is when you have two disjointed sensitivity labels, that is a category in one of the labels is not in the other label. "Because neither label contains all the categories of the other, the labels can't be compared.
They're said to be incomparable"
COMPARABILITY:
The label:
TOP SECRET [VENUS ALPHA]
is "higher" than either of the labels:

SECRET [VENUS ALPHA] TOP SECRET [VENUS]
But you can't really say that the label:
TOP SECRET [VENUS]
is higher than the label:
SECRET [ALPHA]
Because neither label contains all the categories of the other, the labels can't be compared. They're said to be incomparable. In a mandatory access control system, you won't be allowed access to a file whose label is incomparable to your clearance. The Multilevel Security policy uses an ordering relationship between labels known as the dominance relationship. Intuitively, we think of a label that dominates another as being "higher" than the other. Similarly, we think of a label that is dominated by another as being "lower" than the other. The dominance relationship is used to determine permitted operations and information flows.
DOMINANCE
The dominance relationship is determined by the ordering of the Sensitivity/Clearance component of the label and the intersection of the set of Compartments.
Sample Sensitivity/Clearance ordering are:
Top Secret > Secret > Confidential > Unclassified
s3 > s2 > s1 > s0
Formally, for label one to dominate label 2 both of the following must be true:
The sensitivity/clearance of label one must be greater than or equal to the sensitivity/clearance of label two.
The intersection of the compartments of label one and label two must equal the compartments of label two.
Additionally:
Two labels are said to be equal if their sensitivity/clearance and set of compartments are exactly equal. Note that dominance includes equality.
One label is said to strictly dominate the other if it dominates the other but is not equal to the other. Two labels are said to be incomparable if each label has at least one compartment that is not included in the other's set of compartments.
The dominance relationship will produce a partial ordering over all possible MLS labels, resulting in what is known as the MLS Security Lattice.
The following answers are incorrect:
The number of classification in the two labels is different. Is incorrect because the categories are what is being compared, not the classifications.
Neither label contains all the classifications of the other. Is incorrect because the categories are what is being compared, not the classifications.
the number of categories in the two labels is different. Is incorrect because it is possibe a category exists more than once in one sensitivity label and does exist in the other so they would be comparable.
Reference(s) used for this question:
OReilly - Computer Systems and Access Control (Chapter 3) http://www.oreilly.com/catalog/csb/chapter/ch03.html
and
http://rubix.com/cms/mls_dom

QUESTION 5
Which of the following is true about Kerberos?

A. It utilizes public key cryptography.
B. It encrypts data after a ticket is granted, but passwords are exchanged in plain text.
C. It depends upon symmetric ciphers.
D. It is a second party authentication system.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Kerberos depends on secret keys (symmetric ciphers). Kerberos is a third party authentication protocol. It was designed and developed in the mid 1980's by MIT. It is considered open source but is copyrighted and owned by MIT. It relies on the user's secret keys. The password is used to encrypt and decrypt the keys.
The following answers are incorrect:

It utilizes public key cryptography. Is incorrect because Kerberos depends on secret keys (symmetric ciphers). It encrypts data after a ticket is granted, but passwords are exchanged in plain text. Is incorrect because the passwords are not exchanged but used for encryption and decryption of the keys. It is a second party authentication system. Is incorrect because Kerberos is a third party authentication system, you authenticate to the third party (Kerberos) and not the system you are accessing.

MIT http://web.mit.edu/kerberos/
Wikipedi http://en.wikipedia.org/wiki/Kerberos_%28protocol%29 OIG CBK Access Control (pages 181 - 184)
AIOv3 Access Control (pages 151 - 155)

QUESTION 6
Which of the following is needed for System Accountability?

A. Audit mechanisms.
B. Documented design as laid out in the Common Criteria.
C. Authorization.
D. Formal verification of system design.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Is a means of being able to track user actions. Through the use of audit logs and other tools the user actions are recorded and can be used at a later date to verify what actions were performed.
Accountability is the ability to identify users and to be able to track user actions.
The following answers are incorrect:
Documented design as laid out in the Common Criteria. Is incorrect because the Common Criteria is an international standard to evaluate trust and would not be a factor in System Accountability. Authorization. Is incorrect because Authorization is granting access to subjects, just because you have authorization does not hold the subject accountable for their actions. Formal verification of system design. Is incorrect because all you have done is to verify the system design and have not taken any steps toward system accountability.

OIG CBK Glossary (page 778)

QUESTION 7
What is Kerberos?

A. A three-headed dog from the egyptian mythology.
B. A trusted third-party authentication protocol.
C. A security model.
D. A remote authentication dial in user server.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Is correct because that is exactly what Kerberos is.
The following answers are incorrect:
A three-headed dog from Egyptian mythology. Is incorrect because we are dealing with Information Security and not the Egyptian mythology but the Greek Mythology. A security model. Is incorrect because Kerberos is an authentication protocol and not just a security model.
A remote authentication dial in user server. Is incorrect because Kerberos is not a remote authentication dial in user server that would be called RADIUS.

QUESTION 8
The three classic ways of authenticating yourself to the computer security software are by something you know, by something you have, and by something:

A. you need.
B. non-trivial
C. you are.
D. you can get.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: This is more commonly known as biometrics and is one of the most accurate ways to authenticate an individual.
The rest of the answers are incorrect because they not one of the three recognized forms for Authentication.

QUESTION 9
A timely review of system access audit records would be an example of which of the basic security functions?

A. avoidance.
B. deterrence.
C. prevention.
D. detection.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: By reviewing system logs you can detect events that have occured.
The following answers are incorrect:
avoidance. This is incorrect, avoidance is a distractor. By reviewing system logs you have not avoided anything.
deterrence. This is incorrect because system logs are a history of past events. You cannot deter something that has already occurred.
prevention. This is incorrect because system logs are a history of past events. You cannot prevent something that has already occurred.

QUESTION 10
A confidential number used as an authentication factor to verify a user's identity is called a:

A. PIN
B. User ID
C. Password
D. Challenge

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: PIN Stands for Personal Identification Number, as the name states it is a combination of numbers.
The following answers are incorrect:
User ID This is incorrect because a Userid is not required to be a number and a Userid is only used to establish identity not verify it.
Password. This is incorrect because a password is not required to be a number, it could be any combination of characters.
Challenge. This is incorrect because a challenge is not defined as a number, it could be anything.

QUESTION 11
Which of the following exemplifies proper separation of duties?

A. Operators are not permitted modify the system time.
B. Programmers are permitted to use the system console.
C. Console operators are permitted to mount tapes and disks.
D. Tape operators are permitted to use the system console.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: This is an example of Separation of Duties because operators are prevented from modifying the system time which could lead to fraud. Tasks of this nature should be performed by they system administrators.
AIO defines Separation of Duties as a security principle that splits up a critical task among two or more individuals to ensure that one person cannot complete a risky task by himself.
The following answers are incorrect:
Programmers are permitted to use the system console. Is incorrect because programmers should not be permitted to use the system console, this task should be performed by operators. Allowing programmers access to the system console could allow fraud to occur so this is not an example of Separation of Duties..
Console operators are permitted to mount tapes and disks. Is incorrect because operators should be able to mount tapes and disks so this is not an example of Separation of Duties. Tape operators are permitted to use the system console. Is incorrect because operators should be able to use the system console so this is not an example of Separation of Duties.

OIG CBK Access Control (page 98 - 101)
AIOv3 Access Control (page 182)

QUESTION 12
Which of the following is not a logical control when implementing logical access security?

A. access profiles.
B. userids.
C. employee badges.
D. passwords.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Employee badges are considered Physical so would not be a logical control.
The following answers are incorrect:
userids. Is incorrect because userids are a type of logical control. access profiles. Is incorrect because access profiles are a type of logical control. passwords. Is incorrect because passwords are a type of logical control.

QUESTION 13
Which one of the following authentication mechanisms creates a problem for mobile users?

A. Mechanisms based on IP addresses
B. Mechanism with reusable passwords
C. one-time password mechanism.
D. challenge response mechanism.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Anything based on a fixed IP address would be a problem for mobile users because their location and its associated IP address can change from one time to the next. Many providers will assign a new IP every time the device would be restarted. For example an insurance adjuster using a laptop to file claims online. He goes to a different client each time and the address changes every time he connects to the ISP.
NOTE FROM CLEMENT:
The term MOBILE in this case is synonymous with Road Warriors where a user is contantly traveling and changing location. With smartphone today that may not be an issue but it would be an issue for laptops or WIFI tablets. Within a carrier network the IP will tend to be the same and would change rarely. So this question is more applicable to devices that are not cellular devices but in some cases this issue could affect cellular devices as well.
The following answers are incorrect:
mechanism with reusable password. This is incorrect because reusable password mechanism would not present a problem for mobile users. They are the least secure and change only at specific interval.
one-time password mechanism. This is incorrect because a one-time password mechanism would not present a problem for mobile users. Many are based on a clock and not on the IP address of the user.
challenge response mechanism. This is incorrect because challenge response mechanism would not present a problem for mobile users.

QUESTION 14
Organizations should consider which of the following first before allowing external access to their LANs via the Internet?

A. plan for implementing workstation locking mechanisms.
B. plan for protecting the modem pool.
C. plan for providing the user with his account usage information.
D. plan for considering proper authentication options.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Before a LAN is connected to the Internet, you need to determine what the access controls mechanisms are to be used, this would include how you are going to authenticate individuals that may access your network externally through access control.
The following answers are incorrect:
plan for implementing workstation locking mechanisms. This is incorrect because locking the workstations have no impact on the LAN or Internet access. plan for protecting the modem pool. This is incorrect because protecting the modem pool has no impact on the LAN or Internet access, it just protects the modem. plan for providing the user with his account usage information. This is incorrect because the question asks what should be done first. While important your primary concern should be focused on security.

QUESTION 15
Which of the following would assist the most in Host Based intrusion detection?

A. audit trails.
B. access control lists.
C. security clearances.
D. host-based authentication.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: To assist in Intrusion Detection you would review audit logs for access violations.
The following answers are incorrect:

access control lists. This is incorrect because access control lists determine who has access to what but do not detect intrusions.
security clearances. This is incorrect because security clearances determine who has access to what but do not detect intrusions.
host-based authentication. This is incorrect because host-based authentication determine who have been authenticated to the system but do not dectect intrusions.

QUESTION 16
Controls to keep password sniffing attacks from compromising computer systems include which of the following?

A. static and recurring passwords.
B. encryption and recurring passwords.
C. one-time passwords and encryption.
D. static and one-time passwords.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: To minimize the chance of passwords being captured one-time passwords would prevent a password sniffing attack because once used it is no longer valid. Encryption will also minimize these types of attacks.
The following answers are correct:
static and recurring passwords. This is incorrect because if there is no encryption then someone password sniffing would be able to capture the password much easier if it never changed. encryption and recurring passwords. This is incorrect because while encryption helps, recurring passwords do nothing to minimize the risk of passwords being captured. static and one-time passwords. This is incorrect because while one-time passwords will prevent these types of attacks, static passwords do nothing to minimize the risk of passwords being captured.

QUESTION 17
Kerberos can prevent which one of the following attacks?

A. tunneling attack.
B. playback (replay) attack.
C. destructive attack.
D. process attack.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Each ticket in Kerberos has a timestamp and are subject to time expiration to help prevent these types of attacks.
The following answers are incorrect:
tunneling attack. This is incorrect because a tunneling attack is an attempt to bypass security and access low-level systems. Kerberos cannot totally prevent these types of attacks. destructive attack. This is incorrect because depending on the type of destructive attack, Kerberos cannot prevent someone from physically destroying a server. process attack. This is incorrect because with Kerberos cannot prevent an authorzied individuals from running processes.

QUESTION 18
In discretionary access environments, which of the following entities is authorized to grant information access to other people?

A. Manager

B. Group Leader

C. Security Manager

D. Data Owner

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: In Discretionary Access Control (DAC) environments, the user who creates a file is also considered the owner and has full control over the file including the ability to set permissions for that file.
The following answers are incorrect:
manager. Is incorrect because in Discretionary Access Control (DAC) environments it is the owner/user that is authorized to grant information access to other people. group leader. Is incorrect because in Discretionary Access Control (DAC) environments it is the owner/user that is authorized to grant information access to other people. security manager. Is incorrect because in Discretionary Access Control (DAC) environments it is the owner/user that is authorized to grant information access to other people.
IMPORTANT NOTE:
The term Data Owner is also used within Classifications as well. Under the subject of classification the Data Owner is a person from management who has been entrusted with a data set that belongs to the company. For example it could be the Chief Financial Officer (CFO) who is entrusted with all of the financial data for a company. As such the CFO would determine the classification of the financial data and who can access as well. The Data Owner would then tell the Data Custodian (a technical person) what the classification and need to know is on the specific set of data.
The term Data Owner under DAC simply means whoever created the file and as the creator of the file the owner has full access and can grant access to other subjects based on their identity.

QUESTION 19
What is the main concern with single sign-on?

A. Maximum unauthorized access would be possible if a password is disclosed.

B. The security administrator's workload would increase.

C. The users' password would be too hard to remember.

D. User access rights would be increased.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: A major concern with Single Sign-On (SSO) is that if a user's ID and password are compromised, the intruder would have access to all the systems that the user was authorized for.
The following answers are incorrect:
The security administrator's workload would increase. Is incorrect because the security administrator's workload would decrease and not increase. The admin would not be responsible for maintaining multiple user accounts just the one.
The users' password would be too hard to remember. Is incorrect because the users would have less passwords to remember.
User access rights would be increased. Is incorrect because the user access rights would not be any different than if they had to log into systems manually.

QUESTION 20
Who developed one of the first mathematical models of a multilevel-security computer system?

A. Diffie and Hellman.

B. Clark and Wilson.

C. Bell and LaPadula.

D. Gasser and Lipner.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: In 1973 Bell and LaPadula created the first mathematical model of a multi-level security system.
The following answers are incorrect:
Diffie and Hellman. This is incorrect because Diffie and Hellman was involved with cryptography. Clark and Wilson. This is incorrect because Bell and LaPadula was the first model. The Clark- Wilson model came later, 1987.
Gasser and Lipner. This is incorrect, it is a distractor. Bell and LaPadula was the first model.

QUESTION 21
A department manager has read access to the salaries of the employees in his/her department but not to the salaries of employees in other departments. A database security mechanism that enforces this policy would typically be said to provide which of the following?

A. Content-dependent access control
B. Context-dependent access control
C. Least privileges access control
D. Ownership-based access control

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: When access control is based on the content of an object, it is considered to be content dependent access control.
Content-dependent access control is based on the content itself.
The following answers are incorrect:
context-dependent access control. Is incorrect because this type of control is based on what the context is, facts about the data rather than what the object contains. least privileges access control. Is incorrect because this is based on the least amount of rights needed to perform their jobs and not based on what is contained in the database. ownership-based access control. Is incorrect because this is based on the owner of the data and and not based on what is contained in the database.

OIG CBK Access Control (page 191)

QUESTION 22
Which of the following attacks could capture network user passwords?

A. Data diddling
B. Sniffing
C. IP Spoofing
D. Smurfing

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: A network sniffer captures a copy every packet that traverses the network segment the sniffer is connect to.
Sniffers are typically devices that can collect information from a communication medium, such as a network. These devices can range from specialized equipment to basic workstations with customized software.
A sniffer can collect information about most, if not all, attributes of the communication. The most common method of sniffing is to plug a sniffer into an existing network device like a hub or switch. A hub (which is designed to relay all traffic passing through it to all of its ports) will automatically begin sending all the traffic on

that network segment to the sniffing device. On the other hand, a switch (which is designed to limit what traffic gets sent to which port) will have to be specially configured to send all traffic to the port where the sniffer is plugged in. Another method for sniffing is to use a network tap--a device that literally splits a network transmission into two identical streams; one going to the original network destination and the other going to the sniffing device. Each of these methods has its advantages and disadvantages, including cost, feasibility, and the desire to maintain the secrecy of the sniffing activity. The packets captured by sniffer are decoded and then displayed by the sniffer. Therfore, if the username/password are contained in a packet or packets traversing the segment the sniffer is connected to, it will capture and display that information (and any other information on that segment it can see).
Of course, if the information is encrypted via a VPN, SSL, TLS, or similar technology, the information is still captured and displayed, but it is in an unreadable format.
The following answers are incorrect:
Data diddling involves changing data before, as it is enterred into a computer, or after it is extracted.
Spoofing is forging an address and inserting it into a packet to disguise the origin of the communication - or causing a system to respond to the wrong address. Smurfing would refer to the smurf attack, where an attacker sends spoofed packets to the broadcast address on a gateway in order to cause a denial of service.
The following reference(s) were/was used to create this question:
CISA Review manual 2014 Page number 321
Official ISC2 Guide to the CISSP 3rd edition Page Number 153

QUESTION 23
Which of the following would constitute the best example of a password to use for access to a system by a network administrator?

A. holiday
B. Christmas12
C. Jenny
D. GyN19Za!

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: GyN19Za! would be the the best answer because it contains a mixture of upper and lower case characters, alphabetic and numeric characters, and a special character making it less vulnerable to password attacks.
All of the other answers are incorrect because they are vulnerable to brute force or dictionary attacks.
Passwords should not be common words or names. The addition of a number to the end of a common word only marginally strengthens it because a common password attack would also check combinations of words:
Christmas23
Christmas123
etc...

QUESTION 24
The number of violations that will be accepted or forgiven before a violation record is produced is called which of the following?

A. clipping level
B. acceptance level
C. forgiveness level
D. logging level

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The correct answer is "clipping level". This is the point at which a system decides to take some

sort of action when an action repeats a preset number of times. That action may be to log the activity, lock a user account, temporarily close a port, etc. Example: The most classic example of a clipping level is failed login attempts. If you have a system configured to lock a user's account after three failed login attemts, that is the "clipping level".
The other answers are not correct because:
Acceptance level, forgiveness level, and logging level are nonsensical terms that do not exist (to my knowledge) within network security.
Official ISC2 Guide - The term "clipping level" is not in the glossary or index of that book. I cannot find it in the text either. However, I'm quite certain that it would be considered part of the CBK, despite its exclusion from the Official Guide.
All in One Third Edition page: 136 - 137

QUESTION 25
Examples of types of physical access controls include all EXCEPT which of the following?

A. badges
B. locks
C. guards
D. passwords

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Passwords are considered a Preventive/Technical (logical) control.
The following answers are incorrect:
badges Badges are a physical control used to identify an individual. A badge can include a smart device which can be used for authentication and thus a Technical control, but the actual badge itself is primarily a physical control.
locks Locks are a Preventative Physical control and has no Technical association. guards Guards are a Preventative Physical control and has no Technical association. The following reference(s) were/was used to create this question:
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 35).

QUESTION 26
The number of violations that will be accepted or forgiven before a violation record is produced is called which of the following?

A. clipping level
B. acceptance level
C. forgiveness level
D. logging level

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The correct answer is "clipping level". This is the point at which a system decides to take some sort of action when an action repeats a preset number of times. That action may be to log the activity, lock a user account, temporarily close a port, etc. Example: The most classic example of a clipping level is failed login attempts. If you have a system configured to lock a user's account after three failed login attemts, that is the "clipping level".
The other answers are not correct because:
Acceptance level, forgiveness level, and logging level are nonsensical terms that do not exist (to my knowledge) within network security.
Official ISC2 Guide - The term "clipping level" is not in the glossary or index of that book. I cannot find it in the

text either. However, I'm quite certain that it would be considered part of the CBK, despite its exclusion from the Official Guide.
All in One Third Edition page: 136 - 137

QUESTION 27
Examples of types of physical access controls include all EXCEPT which of the following?

A. badges
B. locks
C. guards
D. passwords

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Passwords are considered a Preventive/Technical (logical) control.
The following answers are incorrect:
badges Badges are a physical control used to identify an individual. A badge can include a smart device which can be used for authentication and thus a Technical control, but the actual badge itself is primarily a physical control.
locks Locks are a Preventative Physical control and has no Technical association. guards Guards are a Preventative Physical control and has no Technical association. The following reference(s) were/was used to create this question:
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 35).

QUESTION 28
Guards are appropriate whenever the function required by the security program involves which of the following?

A. The use of discriminating judgment
B. The use of physical force
C. The operation of access control devices
D. The need to detect unauthorized access

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The
Answer: The use of discriminating judgment, a guard can make the determinations that hardware or other automated security devices cannot make due to its ability to adjust to rapidly changing conditions, to learn and alter recognizable patterns, and to respond to various conditions in the environment. Guards are better at making value decisions at times of incidents. They are appropriate whenever immediate, discriminating judgment is required by the security entity.
The following answers are incorrect:
The use of physical force This is not the best answer. A guard provides discriminating judgment, and the ability to discern the need for physical force. The operation of access control devices A guard is often uninvolved in the operations of an automated access control device such as a biometric reader, a smart lock, mantrap, etc. The need to detect unauthorized access The primary function of a guard is not to detect unauthorized access, but to prevent unauthorized physical access attempts and may deter social engineering attempts.
The following reference(s) were/was used to create this question:
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 10: Physical security (page 339).
Source: ISC2 Offical Guide to the CBK page 288-289.

QUESTION 29
What physical characteristic does a retinal scan biometric device measure?

A. The amount of light reaching the retina
B. The amount of light reflected by the retina
C. The pattern of light receptors at the back of the eye
D. The pattern of blood vessels at the back of the eye

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The retina, a thin nerve (1/50th of an inch) on the back of the eye, is the part of the eye which senses light and transmits impulses through the optic nerve to the brain - the equivalent of film in a camera. Blood vessels used for biometric identification are located along the neural retina, the outermost of retina's four cell layers.
The following answers are incorrect:
The amount of light reaching the retina The amount of light reaching the retina is not used in the biometric scan of the retina.
The amount of light reflected by the retina The amount of light reflected by the retina is not used in the biometric scan of the retina.
The pattern of light receptors at the back of the eye This is a distractor The following reference(s) were/was used to create this question:
Retina Scan Technology.
ISC2 Official Guide to the CBK, 2007 (Page 161)

QUESTION 30
Which is the last line of defense in a physical security sense?

A. people
B. interior barriers
C. exterior barriers
D. perimeter barriers

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: "Ultimately, people are the last line of defense for your company's assets" (Pastore & Dulaney, 2006, p. 529).
Pastore, M. and Dulaney, E. (2006). CompTIA Security+ study guide: Exam SY0-101.
Indianapolis, IN: Sybex.

QUESTION 31
The Computer Security Policy Model the Orange Book is based on is which of the following?

A. Bell-LaPadula
B. Data Encryption Standard
C. Kerberos
D. Tempest

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The Computer Security Policy Model Orange Book is based is the Bell-LaPadula Model. Orange

Book Glossary.
The Data Encryption Standard (DES) is a cryptographic algorithm. National Information Security Glossary.
TEMPEST is related to limiting the electromagnetic emanations from electronic equipment. U.S. Department of Defense, Trusted Computer System Evaluation Criteria (Orange Book), DOD 5200.28-STD. December 1985 (also available here).

QUESTION 32
The end result of implementing the principle of least privilege means which of the following?

A. Users would get access to only the info for which they have a need to know
B. Users can access all systems.
C. Users get new privileges added when they change positions.
D. Authorization creep.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The principle of least privilege refers to allowing users to have only the access they need and not anything more. Thus, certain users may have no need to access any of the files on specific systems.
The following answers are incorrect:
Users can access all systems. Although the principle of least privilege limits what access and systems users have authorization to, not all users would have a need to know to access all of the systems. The best answer is still Users would get access to only the info for which they have a need to know as some of the users may not have a need to access a system. Users get new privileges when they change positions. Although true that a user may indeed require new privileges, this is not a given fact and in actuality a user may require less privileges for a new position. The principle of least privilege would require that the rights required for the position be closely evaluated and where possible rights revoked. Authorization creep. Authorization creep occurs when users are given additional rights with new positions and responsibilities. The principle of least privilege should actually prevent authorization creep.
The following reference(s) were/was used to create this question:
ISC2 OIG 2007 p.101,123
Shon Harris AIO v3 p148, 902-903

QUESTION 33
Which of the following is the most reliable authentication method for remote access?

A. Variable callback system
B. Synchronous token
C. Fixed callback system
D. Combination of callback and caller ID

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: A Synchronous token generates a one-time password that is only valid for a short period of time. Once the password is used it is no longer valid, and it expires if not entered in the acceptable time frame.
The following answers are incorrect:
Variable callback system. Although variable callback systems are more flexible than fixed callback systems, the system assumes the identity of the individual unless two-factor authentication is also implemented. By itself, this method might allow an attacker access as a trusted user. Fixed callback system. Authentication provides assurance that someone or something is who or what he/it is supposed to be. Callback systems authenticate a person, but anyone can pretend to be that person. They are tied to a specific place and phone number, which can be spoofed by implementing call-forwarding.
Combination of callback and Caller ID. The caller ID and callback functionality provides greater confidence and auditability of the caller's identity. By disconnecting and calling back only authorized phone numbers, the

system has a greater confidence in the location of the call. However, unless combined with strong authentication, any individual at the location could obtain access.
The following reference(s) were/was used to create this question:
Shon Harris AIO v3 p. 140, 548
ISC2 OIG 2007 p. 152-153, 126-127

QUESTION 34
Which of the following is the most reliable, secure means of removing data from magnetic storage media such as a magnetic tape, or a cassette?

A. Degaussing
B. Parity Bit Manipulation
C. Zeroization
D. Buffer overflow

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: A "Degausser (Otherwise known as a Bulk Eraser) has the main function of reducing to near zero the magnetic flux stored in the magnetized medium. Flux density is measured in Gauss or Tesla. The operation is speedier than overwriting and done in one short operation. This is achieved by subjecting the subject in bulk to a series of fields of alternating polarity and gradually decreasing strength.
The following answers are incorrect:Parity Bit Manipulation. Parity has to do with disk lerror detection, not data removal. A bit or series of bits appended to a character or block of characters to ensure that the information received is the same as the infromation that was sent. Zeroization. Zeroization involves overwrting data to sanitize it. It is time-consuming and not foolproof. The potential of restoration of data does exist with this method. Buffer overflow. This is a detractor. Although many Operating Systems use a disk buffer to temporarily hold data read from disk, its primary purpose has no connection to data removal. An overflow goes outside the constraints defined for the buffer and is a method used by an attacker to attempt access to a system.
The following reference(s) were/was used to create this question:
Shon Harris AIO v3. pg 908
What is degaussing.

QUESTION 35
The Orange Book is founded upon which security policy model?

A. The Biba Model
B. The Bell LaPadula Model
C. Clark-Wilson Model
D. TEMPEST

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: From the glossary of Computer Security Basics:
The Bell-LaPadula model is the security policy model on which the Orange Book requirements are based. From the Orange Book definition, "A formal state transition model of computer security policy that describes a set of access control rules. In this formal model, the entities in a computer system are divided into abstract sets of subjects and objects. The notion of secure state is defined and it is proven that each state transition preserves security by moving from secure state to secure state; thus, inductively proving the system is secure. A system state is defined to be 'secure' if the only permitted access modes of subjects to objects are in accordance with a specific security policy. In order to determine whether or not a specific access mode is allowed, the clearance of a subject is compared to the classification of the object and a determination is made as to whether the subject is authorized for the specific access mode." The Biba Model is an integrity model of computer security policy that describes a set of rules. In this model, a subject may not depend on any object or

other subject that is less trusted than itself. The Clark Wilson Model is an integrity model for computer security policy designed for a commercial environment. It addresses such concepts as nondiscretionary access control, privilege separation, and least privilege. TEMPEST is a government program that prevents the compromising electrical and electromagnetic signals that emanate from computers and related equipment from being intercepted and deciphered.
Source: RUSSEL, Deborah & GANGEMI, G.T. Sr., Computer Security Basics, O'Reilly, 1991. Also: U.S. Department of Defense, Trusted Computer System Evaluation Criteria (Orange Book), DOD 5200.28-STD. December 1985 (also available here).

QUESTION 36
Which of the following is true of two-factor authentication?

A. It uses the RSA public-key signature based on integers with large prime factors.
B. It requires two measurements of hand geometry.
C. It does not use single sign-on technology.
D. It relies on two independent proofs of identity.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The
Answer: It relies on two independent proofs of identity. Two-factor authentication refers to using two independent proofs of identity, such as something the user has (e.g. a token card) and something the user knows (a password). Two-factor authentication may be used with single sign-on.
The following answers are incorrect: It requires two measurements of hand geometry. Measuring hand geometry twice does not yield two independent proofs. It uses the RSA public-key signature based on integers with large prime factors. RSA encryption uses integers with exactly two prime factors, but the term "two-factor authentication" is not used in that context.
It does not use single sign-on technology. This is a detractor. The following reference(s) were/was used to create this question:
Shon Harris AIO v.3 p.129
ISC2 OIG, 2007 p. 126

QUESTION 37
The primary service provided by Kerberos is which of the following?

A. non-repudiation
B. confidentiality
C. authentication
D. authorization

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The
Answer: authentication. Kerberos is an authentication service. It can use singlefactor or multi-factor authentication methods.
The following answers are incorrect:
non-repudiation. Since Kerberos deals primarily with symmetric cryptography, it does not help with non-repudiation.
confidentiality. Once the client is authenticated by Kerberos and obtains its session key and ticket, it may use them to assure confidentiality of its communication with a server; however, that is not a Kerberos service as such.
authorization. Although Kerberos tickets may include some authorization information, the meaning of the authorization fields is not standardized in the Kerberos specifications, and authorization is not a primary

Kerberos service.
The following reference(s) were/was used to create this question:
ISC2 OIG,2007 p. 179-184
Shon Harris AIO v.3 152-155

QUESTION 38
There are parallels between the trust models in Kerberos and Public Key Infrastructure (PKI). When we compare them side by side, Kerberos tickets correspond most closely to which of the following?

A. public keys
B. private keys
C. public-key certificates
D. private-key certificates

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: A Kerberos ticket is issued by a trusted third party. It is an encrypted data structure that includes the service encryption key. In that sense it is similar to a public-key certificate.
However, the ticket is not the key.
The following answers are incorrect:
public keys. Kerberos tickets are not shared out publicly, so they are not like a PKI public key. private keys. Although a Kerberos ticket is not shared publicly, it is not a private key. Private keys are associated with Asymmetric crypto system which is not used by Kerberos. Kerberos uses only the Symmetric crypto system. private key certificates. This is a detractor. There is no such thing as a private key certificate.

QUESTION 39
Which of the following is NOT a system-sensing wireless proximity card?

A. magnetically striped card
B. passive device
C. field-powered device
D. transponder

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, page 342.

QUESTION 40
Which of the following is NOT a type of motion detector?

A. Photoelectric sensor
B. Passive infrared sensors
C. Microwave Sensor.
D. Ultrasonic Sensor.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: A photoelectric sensor does not "directly" sense motion there is a narrow beam that won't set off the sensor unless the beam is broken. Photoelectric sensors, along with dry contact switches, are a type of

perimeter intrusion detector.

All of the other answers are valid types of motion detectors types. The content below on the different types of sensors is from Wikepedia:

Indoor Sensors

These types of sensors are designed for indoor use. Outdoor use would not be advised due to false alarm vulnerability and weather durability.Passive infrared detectors

Passive Infrared Sensor

The passive infrared detector (PIR) is one of the most common detectors found in household and small business environments because it offers affordable and reliable functionality. The term passive means the detector is able to function without the need to generate and radiate its own energy (unlike ultrasonic and microwave volumetric intrusion detectors that are "active" in operation). PIRs are able to distinguish if an infrared emitting object is present by first learning the ambient temperature of the monitored space and then detecting a change in the temperature caused by the presence of an object. Using the principle of differentiation, which is a check of presence or nonpresence, PIRs verify if an intruder or object is actually there. Creating individual zones of detection where each zone comprises one or more layers can achieve differentiation. Between the zones there are areas of no sensitivity (dead zones) that are used by the sensor for comparison.

Ultrasonic detectors

Using frequencies between 15 kHz and 75 kHz, these active detectors transmit ultrasonic sound waves that are inaudible to humans. The Doppler shift principle is the underlying method of operation, in which a change in frequency is detected due to object motion. This is caused when a moving object changes the frequency of sound waves around it. Two conditions must occur to successfully detect a Doppler shift event:

There must be motion of an object either towards or away from the receiver. The motion of the object must cause a change in the ultrasonic frequency to the receiver relative to the transmitting frequency.

The ultrasonic detector operates by the transmitter emitting an ultrasonic signal into the area to be protected. The sound waves are reflected by solid objects (such as the surrounding floor, walls and ceiling) and then detected by the receiver. Because ultrasonic waves are transmitted through air, then hard-surfaced objects tend to reflect most of the ultrasonic energy, while soft surfaces tend to absorb most energy.

When the surfaces are stationary, the frequency of the waves detected by the receiver will be equal to the transmitted frequency. However, a change in frequency will occur as a result of the Doppler principle, when a person or object is moving towards or away from the detector. Such an event initiates an alarm signal. This technology is considered obsolete by many alarm professionals, and is not actively installed.

Microwave detectors

This device emits microwaves from a transmitter and detects any reflected microwaves or reduction in beam intensity using a receiver. The transmitter and receiver are usually combined inside a single housing (monostatic) for indoor applications, and separate housings (bistatic) for outdoor applications. To reduce false alarms this type of detector is usually combined with a passive infrared detector or "Dualtec" alarm.

Microwave detectors respond to a Doppler shift in the frequency of the reflected energy, by a phase shift, or by a sudden reduction of the level of received energy. Any of these effects may indicate motion of an intruder.

Photo-electric beams

Photoelectric beam systems detect the presence of an intruder by transmitting visible or infrared light beams across an area, where these beams may be obstructed. To improve the detection surface area, the beams are often employed in stacks of two or more. However, if an intruder is aware of the technology's presence, it can be avoided. The technology can be an effective longrange detection system, if installed in stacks of three or more where the transmitters and receivers are staggered to create a fence-like barrier. Systems are available for both internal and external applications. To prevent a clandestine attack using a secondary light source being used to hold the detector in a 'sealed' condition whilst an intruder passes through, most systems use and detect a modulated light source.

Glass break detectors

The glass break detector may be used for internal perimeter building protection. When glass breaks it generates sound in a wide band of frequencies. These can range from infrasonic, which is below 20 hertz (Hz) and can not be heard by the human ear, through the audio band from 20 Hz to 20 kHz which humans can hear, right up to ultrasonic, which is above 20 kHz and again cannot be heard. Glass break acoustic detectors are mounted in close proximity to the glass panes and listen for sound frequencies associated with glass breaking. Seismic glass break detectors are different in that they are installed on the glass pane. When glass breaks it produces specific shock frequencies which travel through the glass and often through the window frame and the surrounding walls and ceiling. Typically, the most intense frequencies generated are between 3 and 5 kHz, depending on the type of glass and the presence of a plastic interlayer. Seismic glass break detectors "feel" these shock frequencies and in turn generate an alarm condition. The more primitive detection method involves gluing a thin strip of conducting foil on the inside of the glass and putting low-power electrical current through it. Breaking the glass is practically guaranteed to tear the foil and break the circuit.

Smoke, heat, and carbon monoxide detectors

Heat Detection System

Most systems may also be equipped with smoke, heat, and/or carbon monoxide detectors. These are also known as 24 hour zones (which are on at all times). Smoke detectors and heat detectors protect from the risk of fire and carbon monoxide detectors protect from the risk of carbon monoxide. Although an intruder alarm panel may also have these detectors connected, it may not meet all the local fire code requirements of a fire alarm system.

Other types of volumetric sensors could be:

Active Infrared
Passive Infrared/Microware combined
Radar
Accoustical Sensor/Audio
Vibration Sensor (seismic)
Air Turbulence

QUESTION 41
Which of the following is NOT a technique used to perform a penetration test?

A. traffic padding
B. scanning and probing
C. war dialing
D. sniffing

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Traffic padding is a countermeasure to traffic analysis. Even if perfect cryptographic routines are used, the attacker can gain knowledge of the amount of traffic that was generated. The attacker might not know what Alice and Bob were talking about, but can know that they were talking and how much they talked. In certain circumstances this can be very bad. Consider for example when a military is organising a secret attack against another nation: it may suffice to alert the other nation for them to know merely that there is a lot of secret activity going on.
As another example, when encrypting Voice Over IP streams that use variable bit rate encoding, the number of bits per unit of time is not obscured, and this can be exploited to guess spoken phrases.
Padding messages is a way to make it harder to do traffic analysis. Normally, a number of random bits are appended to the end of the message with an indication at the end how much this random data is. The randomness should have a minimum value of 0, a maximum number of N and an even distribution between the two extremes. Note, that increasing 0 does not help, only increasing N helps, though that also means that a lower percentage of the channel will be used to transmit real data. Also note, that since the cryptographic routine is assumed to be uncrackable (otherwise the padding length itself is crackable), it does not help to put the padding anywhere else, e.g. at the beginning, in the middle, or in a sporadic manner. The other answers are all techniques used to do Penetration Testing.

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, pages 233, 238.
and
https://secure.wikimedia.org/wikipedia/en/wiki/Padding_%28cryptography%29#Traffic_analysis

QUESTION 42
In which of the following model are Subjects and Objects identified and the permissions applied to each subject/object combination are specified. Such a model can be used to quickly summarize what permissions a subject has for various system objects.

A. Access Control Matrix model
B. Take-Grant model
C. Bell-LaPadula model
D. Biba model

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: An access control matrix is a table of subjects and objects indicating what actions individual subjects can take upon individual objects. Matrices are data structures that programmers implement as table

lookups that will be used and enforced by the operating system. This type of access control is usually an attribute of DAC models. The access rights can be assigned directly to the subjects (capabilities) or to the objects (ACLs).
Capability Table
A capability table specifies the access rights a certain subject possesses pertaining to specific objects. A capability table is different from an ACL because the subject is bound to the capability table, whereas the object is bound to the ACL.
Access control lists (ACLs)
ACLs are used in several operating systems, applications, and router configurations. They are lists of subjects that are authorized to access a specific object, and they define what level of authorization is granted. Authorization can be specific to an individual, group, or role. ACLs map values from the access control matrix to the object.
Whereas a capability corresponds to a row in the access control matrix, the ACL corresponds to a column of the matrix.
NOTE: Ensure you are familiar with the terms Capability and ACLs for the purpose of the exam.
Resource(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 5264- 5267). McGraw-Hill. Kindle Edition.
or
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition, Page 229 and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 1923-1925). Auerbach Publications. Kindle Edition.

QUESTION 43
In which of the following security models is the subject's clearance compared to the object's classification such that specific rules can be applied to control how the subject-to-object interactions take place?

A. Bell-LaPadula model
B. Biba model
C. Access Matrix model
D. Take-Grant model

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The Bell-LAPadula model is also called a multilevel security system because users with different clearances use the system and the system processes data with different classifications. Developed by the US Military in the 1970s. A security model maps the abstract goals of the policy to information system terms by specifying explicit data structures and techniques necessary to enforce the security policy. A security model is usually represented in mathematics and analytical ideas, which are mapped to system specifications and then developed by programmers through programming code. So we have a policy that encompasses security goals, such as "each subject must be authenticated and authorized before accessing an object." The security model takes this requirement and provides the necessary mathematical formulas, relationships, and logic structure to be followed to accomplish this goal.
A system that employs the Bell-LaPadula model is called a multilevel security system because users with different clearances use the system, and the system processes data at different classification levels. The level at which information is classified determines the handling procedures that should be used. The Bell-LaPadula model is a state machine model that enforces the confidentiality aspects of access control. A matrix and security levels are used to determine if subjects can access different objects. The subject's clearance is compared to the object's classification and then specific rules are applied to control how subject-to-object subject-to-object interactions can take place.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 369). McGraw-Hill.
Kindle Edition.

QUESTION 44
Which of the following classes is the first level (lower) defined in the TCSEC (Orange Book) as mandatory

protection?

A. B
B. A
C. C
D. D

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: B level is the first Mandatory Access Control Level. First published in 1983 and updated in 1985, the TCSEC, frequently referred to as the Orange Book, was a United States Government Department of Defense (DoD) standard that sets basic standards for the implementation of security protections in computing systems. Primarily intended to help the DoD find products that met those basic standards, TCSEC was used to evaluate, classify, and select computer systems being considered for the processing, storage, and retrieval of sensitive or classified information on military and government systems. As such, it was strongly focused on enforcing confidentiality with no focus on other aspects of security such as integrity or availability. Although it has since been superseded by the common criteria, it influenced the development of other product evaluation criteria, and some of its basic approach and terminology continues to be used.
Reference used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 17920-17926). Auerbach Publications. Kindle Edition.
and THE source for all TCSEC "level" questions:
http://csrc.nist.gov/publications/secpubs/rainbow/std001.txt (paragraph 3 for this one)

QUESTION 45
Which of the following classes is defined in the TCSEC (Orange Book) as discretionary protection?

A. C
B. B
C. A
D. D

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, page 197.
Also: THE source for all TCSEC "level" questions:
http://csrc.nist.gov/publications/secpubs/rainbow/std001.txt

QUESTION 46
Which of the following division is defined in the TCSEC (Orange Book) as minimal protection?

A. Division D
B. Division C
C. Division B
D. Division A

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The criteria are divided into four divisions: D, C, B, and A ordered in a hierarchical manner with

the highest division (A) being reserved for systems providing the most comprehensive security.
Each division represents a major improvement in the overall confidence one can place in the system for the protection of sensitive information.
Within divisions C and B there are a number of subdivisions known as classes. The classes are also ordered in a hierarchical manner with systems representative of division C and lower classes of division B being characterized by the set of computer security mechanisms that they possess. Assurance of correct and complete design and implementation for these systems is gained mostly through testing of the security-relevant portions of the system. The security-relevant portions of a system are referred to throughout this document as the Trusted Computing Base (TCB). Systems representative of higher classes in division B and division A derive their security attributes more from their design and implementation structure. Increased assurance that the required features are operative, correct, and tamperproof under all circumstances is gained through progressively more rigorous analysis during the design process. TCSEC provides a classification system that is divided into hierarchical divisions of assurance levels:
Division D - minimal security
Division C - discretionary protection
Division B - mandatory protection
Division A - verified protection
page 358 AIO V.5 Shon Harris
also
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, page 197.
Also:
THE source for all TCSEC "level" questions:
http://csrc.nist.gov/publications/secpubs/rainbow/std001.txt

QUESTION 47
Which of the following was developed by the National Computer Security Center (NCSC) for the US Department of Defense ?

A. TCSEC

B. ITSEC

C. DIACAP

D. NIACAP

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The
Answer: TCSEC; The TCSEC, frequently referred to as the Orange Book, is the centerpiece of the DoD Rainbow Series publications.
Initially issued by the National Computer Security Center (NCSC) an arm of the National Security Agency in 1983 and then updated in 1985, TCSEC was replaced with the development of the Common Criteria international standard originally published in 2005.

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, pages 197-199.
Wikepedia
http://en.wikipedia.org/wiki/TCSEC

QUESTION 48
Which of the following was developed to address some of the weaknesses in Kerberos and uses public key cryptography for the distribution of secret keys and provides additional access control support?

A. SESAME

B. RADIUS

C. KryptoKnight

D. TACACS+

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Secure European System for Applications in a Multi-vendor Environment (SESAME) was developed to address some of the weaknesses in Kerberos and uses public key cryptography for the distribution of secret keys and provides additional access control support. TIPTON, Harold, Official (ISC)2 Guide to the CISSP CBK (2007), page 184.
ISC OIG Second Edition, Access Controls, Page 111

QUESTION 49
Single Sign-on (SSO) is characterized by which of the following advantages?

A. Convenience
B. Convenience and centralized administration
C. Convenience and centralized data administration
D. Convenience and centralized network administration

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Convenience -Using single sign-on users have to type their passwords only once when they first log in to access all the network resources; and Centralized Administration as some single sign-on systems are built around a unified server administration system. This allows a single administrator to add and delete accounts across the entire network from one user interface.
The following answers are incorrect:
Convenience - alone this is not the correct answer.
Centralized Data or Network Administration - these are thrown in to mislead the student. Neither are a benefit to SSO, as these specifically should not be allowed with just an SSO. TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, page 35.
TIPTON, Harold F. & HENRY, Kevin, Official (ISC)2 Guide to the CISSP CBK, 2007, page 180.

QUESTION 50
The "vulnerability of a facility" to damage or attack may be assessed by all of the following except:

A. Inspection
B. History of losses
C. Security controls
D. security budget

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Source: The CISSP Examination Textbook- Volume 2: Practice by S. Rao Vallabhaneni.

QUESTION 51
What is the primary role of smartcards in a PKI?

A. Transparent renewal of user keys
B. Easy distribution of the certificates between the users
C. Fast hardware encryption of the raw data

D. Tamper resistant, mobile storage and application of private keys of the users

Correct Answer: D
Explanation

Explanation/Reference:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw- Hill/Osborne, page 139;
SNYDER, J., What is a SMART CARD?.
Wikipedia has a nice definition at: http://en.wikipedia.org/wiki/Tamper_resistance Security
Tamper-resistant microprocessors are used to store and process private or sensitive information, such as private keys or electronic money credit. To prevent an attacker from retrieving or modifying the information, the chips are designed so that the information is not accessible through external means and can be accessed only by the embedded software, which should contain the appropriate security measures.
Examples of tamper-resistant chips include all secure cryptoprocessors, such as the IBM 4758 and chips used in smartcards, as well as the Clipper chip. It has been argued that it is very difficult to make simple electronic devices secure against tampering, because numerous attacks are possible, including:
physical attack of various forms (microprobing, drills, files, solvents, etc.) freezing the device
applying out-of-spec voltages or power surges
applying unusual clock signals
inducing software errors using radiation
measuring the precise time and power requirements of certain operations (see power analysis) Tamper-resistant chips may be designed to zeroise their sensitive data (especially cryptographic keys) if they detect penetration of their security encapsulation or out-of-specification environmental parameters. A chip may even be rated for "cold zeroisation", the ability to zeroise itself even after its power supply has been crippled. Nevertheless, the fact that an attacker may have the device in his possession for as long as he likes, and perhaps obtain numerous other samples for testing and practice, means that it is practically impossible to totally eliminate tampering by a sufficiently motivated opponent. Because of this, one of the most important elements in protecting a system is overall system design. In particular, tamper-resistant systems should "fail gracefully" by ensuring that compromise of one device does not compromise the entire system. In this manner, the attacker can be practically restricted to attacks that cost less than the expected return from compromising a single device (plus, perhaps, a little more for kudos). Since the most sophisticated attacks have been estimated to cost several hundred thousand dollars to carry out, carefully designed systems may be invulnerable in practice.

QUESTION 52
What kind of certificate is used to validate a user identity?

A. Public key certificate
B. Attribute certificate
C. Root certificate
D. Code signing certificate

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: In cryptography, a public key certificate (or identity certificate) is an electronic document which incorporates a digital signature to bind together a public key with an identity -- information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual. In a typical public key infrastructure (PKI) scheme, the signature will be of a certificate authority (CA). In a web of trust scheme, the signature is of either the user (a self-signed certificate) or other users ("endorsements"). In either case, the signatures on a certificate are attestations by the certificate signer that the identity information and the public key belong together. In computer security, an authorization certificate (also known as an attribute certificate) is a digital document that describes a written permission from the issuer to use a service or a resource that the issuer controls or has access to use. The permission can be delegated. Some people constantly confuse PKCs and ACs. An analogy may make the distinction clear. A PKC can be considered to be like a passport: it identifies the holder, tends to last for a long time, and should not be trivial to obtain. An AC is more like an entry visa: it is typically issued by a different authority and does

not last for as long a time. As acquiring an entry visa typically requires presenting a passport, getting a visa can be a simpler process. A real life example of this can be found in the mobile software deployments by large service providers and are typically applied to platforms such as Microsoft Smartphone (and related), Symbian OS, J2ME, and others.
In each of these systems a mobile communications service provider may customize the mobile terminal client distribution (ie. the mobile phone operating system or application environment) to include one or more root certificates each associated with a set of capabilities or permissions such as "update firmware", "access address book", "use radio interface", and the most basic one, "install and execute". When a developer wishes to enable distribution and execution in one of these controlled environments they must acquire a certificate from an appropriate CA, typically a large commercial CA, and in the process they usually have their identity verified using out-of-band mechanisms such as a combination of phone call, validation of their legal entity through government and commercial databases, etc., similar to the high assurance SSL certificate vetting process, though often there are additional specific requirements imposed on would-be developers/publishers.
Once the identity has been validated they are issued an identity certificate they can use to sign their software; generally the software signed by the developer or publisher's identity certificate is not distributed but rather it is submitted to processor to possibly test or profile the content before generating an authorization certificate which is unique to the particular software release. That certificate is then used with an ephemeral asymmetric key-pair to sign the software as the last step of preparation for distribution. There are many advantages to separating the identity and authorization certificates especially relating to risk mitigation of new content being accepted into the system and key management as well as recovery from errant software which can be used as attack vectors.

HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw-Hill/Osborne, page 540.
http://en.wikipedia.org/wiki/Attribute_certificate
http://en.wikipedia.org/wiki/Public_key_certificate

QUESTION 53
Which of the following is not a physical control for physical security?

A. lighting
B. fences
C. training
D. facility construction materials

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Some physical controls include fences, lights, locks, and facility construction materials. Some administrative controls include facility selection and construction, facility management, personnel controls, training, and emergency response and procedures. From: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 3rd.
Ed., Chapter 6, page 403.

QUESTION 54
Crime Prevention Through Environmental Design (CPTED) is a discipline that:

A. Outlines how the proper design of a physical environment can reduce crime by directly affecting human behavior.
B. Outlines how the proper design of the logical environment can reduce crime by directly affecting human behavior.
C. Outlines how the proper design of the detective control environment can reduce crime by directly affecting human behavior.
D. Outlines how the proper design of the administrative control environment can reduce crime by directly affecting human behavior.

Correct Answer: A

Explanation

Explanation/Reference:
Explanation: Crime Prevention Through Environmental Design (CPTED) is a discipline that outlines how the proper design of a physical environment can reduce crime by directly affecting human behavior. It provides guidance about lost and crime prevention through proper facility contruction and environmental components and procedures. CPTED concepts were developed in the 1960s. They have been expanded upon and have matured as our environments and crime types have evolved. CPTED has been used not just to develop corporate physical security programs, but also for large-scale activities such as development of neighborhoods, towns, and cities. It addresses landscaping, entrances, facility and neighborhood layouts, lighting, road placement, and traffic circulation patterns. It looks at microenvironments, such as offices and rest-rooms, and macroenvironments, like campuses and cities.
Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 435). McGraw-Hill.
Kindle Edition.
and
CPTED Guide Book

QUESTION 55
The following is NOT a security characteristic we need to consider while choosing a biometric identification systems:

A. data acquisition process
B. cost
C. enrollment process
D. speed and user interface

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Cost is a factor when considering Biometrics but it is not a security characteristic. All the other answers are incorrect because they are security characteristics related to Biometrics. data acquisition process can cause a security concern because if the process is not fast and efficient it can discourage individuals from using the process. enrollment process can cause a security concern because the enrollment process has to be quick and efficient. This process captures data for authentication. speed and user interface can cause a security concern because this also impacts the users acceptance rate of biometrics. If they are not comfortable with the interface and speed they might sabotage the devices or otherwise attempt to circumvent them.

OIG Access Control (Biometrics) (pgs 165-167)
From: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, Pages 5-6.
in process of correction

QUESTION 56
In biometric identification systems, at the beginning, it was soon apparent that truly positive identification could only be based on :

A. sex of a person
B. physical attributes of a person
C. age of a person
D. voice of a person

Correct Answer: B
Explanation

Explanation/Reference:

Explanation: Today implementation of fast, accurate reliable and user-acceptable biometric identification systems is already under way.
From: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, Page 7.

QUESTION 57
In biometric identification systems, at the beginning, it was soon apparent that truly positive identification could only be based on physical attributes of a person. This raised the necessity of answering 2 questions :

A. what was the sex of a person and his age
B. what part of body to be used and how to accomplish identification that is viable
C. what was the age of a person and his income level
D. what was the tone of the voice of a person and his habits

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Today implementation of fast, accurate reliable and user-acceptable biometric identification systems is already taking place. Unique physical attributes or behavior of a person are used for that purpose.
From: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, Page 7.

QUESTION 58
In biometric identification systems, the parts of the body conveniently available for identification are:

A. neck and mouth
B. hands, face, and eyes
C. feet and hair
D. voice and neck

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Today implementation of fast, accurate, reliable, and user-acceptable biometric identification systems are already under way. Because most identity authentication takes place when a people are fully clothed (neck to feet and wrists), the parts of the body conveniently available for this purpose are hands, face, and eyes.
From: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, Page 7.

QUESTION 59
Controlling access to information systems and associated networks is necessary for the preservation of their:

A. Authenticity, confidentiality and availability
B. Confidentiality, integrity, and availability.
C. integrity and availability.
D. authenticity,confidentiality, integrity and availability.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Controlling access to information systems and associated networks is necessary for the preservation of their confidentiality, integrity and availability. Source: KRUTZ, Ronald L. & VINES, Russel D.,

The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 31.

QUESTION 60
Controls like guards and general steps to maintain building security, securing of server rooms or laptops, the protection of cables, and usage of magnetic switches on doors and windows are some of the examples of:

A. Administrative controls
B. Logical controls
C. Technical controls
D. Physical controls

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Controls like guards and general steps to maintain building security, securing of server rooms or laptops, the protection of cables, and usage of magnetic switches on doors and windows are all examples of Physical Security.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

QUESTION 61
To control access by a subject (an active entity such as individual or process) to an object (a passive entity such as a file) involves setting up:

A. Access Rules
B. Access Matrix
C. Identification controls
D. Access terminal

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Controlling access by a subject (an active entity such as individual or process) to an object (a passive entity such as a file) involves setting up access rules. These rules can be classified into three access control models: Mandatory, Discretionary, and Non-Discretionary.
An access matrix is one of the means used to implement access control. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

QUESTION 62
Rule-Based Access Control (RuBAC) access is determined by rules. Such rules would fit within what category of access control ?

A. Discretionary Access Control (DAC)
B. Mandatory Access control (MAC)
C. Non-Discretionary Access Control (NDAC)
D. Lattice-based Access control

Correct Answer: C
Explanation

Explanation/Reference:

Explanation: Rule-based access control is a type of non-discretionary access control because this access is determined by rules and the subject does not decide what those rules will be, the rules are uniformly applied to ALL of the users or subjects. In general, all access control policies other than DAC are grouped in the category of nondiscretionary access control (NDAC). As the name implies, policies in this category have rules that are not established at the discretion of the user. Non-discretionary policies establish controls that cannot be changed by users, but only through administrative action. Both Role Based Access Control (RBAC) and Rule Based Access Control (RuBAC) fall within Non Discretionary Access Control (NDAC). If it is not DAC or MAC then it is most likely NDAC.

IT IS NOT ALWAYS BLACK OR WHITE

The different access control models are not totally exclusive of each others. MAC is making use of Rules to be implemented. However with MAC you have requirements above and beyond having simple access rules. The subject would get formal approval from management, the subject must have the proper security clearance, objects must have labels/sensitivity levels attached to them, subjects must have the proper security clearance. If all of this is in place then you have MAC. BELOW YOU HAVE A DESCRIPTION OF THE DIFFERENT CATEGORIES:

MAC = Mandatory Access Control

Under a mandatory access control environment, the system or security administrator will define what permissions subjects have on objects. The administrator does not dictate user's access but simply configure the proper level of access as dictated by the Data Owner. The MAC system will look at the Security Clearance of the subject and compare it with the object sensitivity level or classification level. This is what is called the dominance relationship. The subject must DOMINATE the object sensitivity level. Which means that the subject must have a security clearance equal or higher than the object he is attempting to access. MAC also introduce the concept of labels. Every objects will have a label attached to them indicating the classification of the object as well as categories that are used to impose the need to know (NTK) principle. Even thou a user has a security clearance of Secret it does not mean he would be able to access any Secret documents within the system. He would be allowed to access only Secret document for which he has a Need To Know, formal approval, and object where the user belong to one of the categories attached to the object. If there is no clearance and no labels then IT IS NOT Mandatory Access Control. Many of the other models can mimic MAC but none of them have labels and a dominance relationship so they are NOT in the MAC category.

NISTR-7316 Says:

Usually a labeling mechanism and a set of interfaces are used to determine access based on the MAC policy; for example, a user who is running a process at the Secret classification should not be allowed to read a file with a label of Top Secret. This is known as the "simple security rule," or "no read up." Conversely, a user who is running a process with a label of Secret should not be allowed to write to a file with a label of Confidential. This rule is called the "*-property" (pronounced "star property") or "no write down." The *-property is required to maintain system security in an automated environment. A variation on this rule called the "strict *-property" requires that information can be written at, but not above, the subject's clearance level. Multilevel security models such as the Bell-La Padula Confidentiality and Biba Integrity models are used to formally specify this kind of MAC policy.

DAC = Discretionary Access Control

DAC is also known as: Identity Based access control system. The owner of an object is define as the person who created the object. As such the owner has the discretion to grant access to other users on the network. Access will be granted based solely on the identity of those users.

Such system is good for low level of security. One of the major problem is the fact that a user who has access to someone's else file can further share the file with other users without the knowledge or permission of the owner of the file. Very quickly this could become the wild wild west as there is no control on the dissimination of the information.

RBAC = Role Based Access Control

RBAC is a form of Non-Discretionary access control.

Role Based access control usually maps directly with the different types of jobs performed by employees within a company.

For example there might be 5 security administrator within your company. Instead of creating each of their profile one by one, you would simply create a role and assign the administrators to the role. Once an administrator has been assigned to a role, he will IMPLICITLY inherit the permissions of that role.

RBAC is great tool for environment where there is a a large rotation of employees on a daily basis such as a very large help desk for example.

RBAC or RuBAC = Rule Based Access Control

RuBAC is a form of Non-Discretionary access control.

A good example of a Rule Based access control device would be a Firewall. A single set of rules is imposed to

all users attempting to connect through the firewall.
NOTE FROM CLEMENT:
Lot of people tend to confuse MAC and Rule Based Access Control. Mandatory Access Control must make use of LABELS. If there is only rules and no label, it cannot be Mandatory Access Control. This is why they call it Non Discretionary Access control (NDAC). There are even books out there that are WRONG on this subject. Books are sometimes opiniated and not strictly based on facts.
In MAC subjects must have clearance to access sensitive objects. Objects have labels that contain the classification to indicate the sensitivity of the object and the label also has categories to enforce the need to know.
Today the best example of rule based access control would be a firewall. All rules are imposed globally to any user attempting to connect through the device. This is NOT the case with MAC. I strongly recommend you read carefully the following document:
NISTIR-7316 at http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf It is one of the best Access Control Study document to prepare for the exam. Usually I tell people not to worry about the hundreds of NIST documents and other reference. This document is an exception. Take some time to read it.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.
and
NISTIR-7316 at http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf and
Conrad, Eric; Misenar, Seth; Feldman, Joshua (2012-09-01). CISSP Study Guide (Kindle Locations 651-652). Elsevier Science (reference). Kindle Edition.

QUESTION 63
The type of discretionary access control (DAC) that is based on an individual's identity is also called:

A. Identity-based Access control
B. Rule-based Access control
C. Non-Discretionary Access Control
D. Lattice-based Access control

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: An identity-based access control is a type of Discretionary Access Control (DAC) that is based on an individual's identity.
DAC is good for low level security environment. The owner of the file decides who has access to the file.
If a user creates a file, he is the owner of that file. An identifier for this user is placed in the file header and/or in an access control matrix within the operating system. Ownership might also be granted to a specific individual. For example, a manager for a certain department might be made the owner of the files and resources within her department. A system that uses discretionary access control (DAC) enables the owner of the resource to specify which subjects can access specific resources.
This model is called discretionary because the control of access is based on the discretion of the owner. Many times department managers, or business unit managers , are the owners of the data within their specific department. Being the owner, they can specify who should have access and who should not.
Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 220). McGraw-Hill .
Kindle Edition.

QUESTION 64
Which access control type has a central authority that determine to what objects the subjects have access to and it is based on role or on the organizational security policy?

A. Mandatory Access Control
B. Discretionary Access Control
C. Non-Discretionary Access Control

D. Rule-based Access control

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Non Discretionary Access Control include Role Based Access Control (RBAC) and Rule Based Access Control (RBAC or RuBAC). RABC being a subset of NDAC, it was easy to eliminate RBAC as it was covered under NDAC already.
Some people think that RBAC is synonymous with NDAC but RuBAC would also fall into this category.
Discretionary Access control is for environment with very low level of security. There is no control on the dissemination of the information. A user who has access to a file can copy the file or further share it with other users.
Rule Based Access Control is when you have ONE set of rules applied uniformly to all users. A good example would be a firewall at the edge of your network. A single rule based is applied against any packets received from the internet.
Mandatory Access Control is a very rigid type of access control. The subject must dominate the object and the subject must have a Need To Know to access the information. Objects have labels that indicate the sensitivity (classification) and there is also categories to enforce the Need To Know (NTK).
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

QUESTION 65
What is called the type of access control where there are pairs of elements that have the least upper bound of values and greatest lower bound of values?

A. Mandatory model
B. Discretionary model
C. Lattice model
D. Rule model

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: In a lattice model, there are pairs of elements that have the least upper bound of values and greatest lower bound of values.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.

QUESTION 66
Which of the following control pairing places emphasis on "soft" mechanisms that support the access control objectives?

A. Preventive/Technical Pairing
B. Preventive/Administrative Pairing
C. Preventive/Physical Pairing
D. Detective/Administrative Pairing

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Soft Control is another way of referring to Administrative control. Technical and Physical controls are NOT soft control, so any choice listing them was not the best answer.
Preventative/Technical is incorrect because although access control can be technical control, it is commonly

not referred to as a "soft" control
Preventative/Administrative is correct because access controls are preventative in nature. it is always best to prevent a negative event, however there are times where controls might fail and you cannot prevent everything. Administrative controls are roles, responsibilities, policies, etc which are usually paper based. In the administrative category you would find audit, monitoring, and security awareness as well.
Preventative/Physical pairing is incorrect because Access controls with an emphasis on "soft" mechanisms conflict with the basic concept of physical controls, physical controls are usually tangible objects such as fences, gates, door locks, sensors, etc... Detective/Administrative Pairing is incorrect because access control is a preventative control used to control access, not to detect violations to access. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.

QUESTION 67
Which of the following control pairings include: organizational policies and procedures, preemployment background checks, strict hiring practices, employment agreements, employee termination procedures, vacation scheduling, labeling of sensitive materials, increased supervision, security awareness training, behavior awareness, and sign-up procedures to obtain access to information systems and networks?

A. Preventive/Administrative Pairing
B. Preventive/Technical Pairing
C. Preventive/Physical Pairing
D. Detective/Administrative Pairing

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The
Answer: Preventive/Administrative Pairing: These mechanisms include organizational policies and procedures, pre-employment background checks, strict hiring practices, employment agreements, friendly and unfriendly employee termination procedures, vacation scheduling, labeling of sensitive materials, increased supervision, security awareness training, behavior awareness, and sign-up procedures to obtain access to information systems and networks.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.

QUESTION 68
Technical controls such as encryption and access control can be built into the operating system, be software applications, or can be supplemental hardware/software units. Such controls, also known as logical controls, represent which pairing?

A. Preventive/Administrative Pairing
B. Preventive/Technical Pairing
C. Preventive/Physical Pairing
D. Detective/Technical Pairing

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Preventive/Technical controls are also known as logical controls and can be built into the operating system, be software applications, or can be supplemental hardware/software units.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.

QUESTION 69
What is called the use of technologies such as fingerprint, retina, and iris scans to authenticate the individuals

requesting access to resources?

A. Micrometrics
B. Macrometrics
C. Biometrics
D. MicroBiometrics

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 35.

QUESTION 70
What are called user interfaces that limit the functions that can be selected by a user?

A. Constrained user interfaces
B. Limited user interfaces
C. Mini user interfaces
D. Unlimited user interfaces

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Constrained user interfaces limit the functions that can be selected by a user. Another method for controlling access is by restricting users to specific functions based on their role in the system. This is typically implemented by limiting available menus, data views, encryption, or by physically constraining the user interfaces. This is common on devices such as an automated teller machine (ATM). The advantage of a constrained user interface is that it limits potential avenues of attack and system failure by restricting the processing options that are available to the user. On an ATM machine, if a user does not have a checking account with the bank he or she will not be shown the "Withdraw money from checking" option. Likewise, an information system might have an "Add/Remove Users" menu option for administrators, but if a normal, non-administrative user logs in he or she will not even see that menu option. By not even identifying potential options for non-qualifying users, the system limits the potentially harmful execution of unauthorized system or application commands.
Many database management systems have the concept of "views." A database view is an extract of the data stored in the database that is filtered based on predefined user or system criteria. This permits multiple users to access the same database while only having the ability to access data they need (or are allowed to have) and not data for another user. The use of database views is another example of a constrained user interface.
The following were incorrect answers:
All of the other choices presented were bogus answers. The following reference(s) were used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 1989-2002). Auerbach Publications. Kindle Edition.

QUESTION 71
What would be the name of a Logical or Virtual Table dynamically generated to restrict the information a user can access in a database?

A. Database Management system
B. Database views
C. Database security
D. Database shadowing

Correct Answer: B

Explanation

Explanation/Reference:
Explanation: The
Answer: Database views; Database views are mechanisms that restrict access to the information that a user can access in a database.Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 35.
Wikipedia has a detailed explantion as well:
In database theory, a view is a virtual or logical table composed of the result set of a query. Unlike ordinary tables (base tables) in a relational database, a view is not part of the physical schema: it is a dynamic, virtual table computed or collated from data in the database. Changing the data in a table alters the data shown in the view.
Views can provide advantages over tables;
They can subset the data contained in a table
They can join and simplify multiple tables into a single virtual table Views can act as aggregated tables, where aggregated data (sum, average etc.) are calculated and presented as part of the data
Views can hide the complexity of data, for example a view could appear as Sales2000 or Sales2001, transparently partitioning the actual underlying table Views do not incur any extra storage overhead
Depending on the SQL engine used, views can provide extra security. Limit the exposure to which a table or tables are exposed to outer world Just like functions (in programming) provide abstraction, views can be used to create abstraction. Also, just like functions, views can be nested, thus one view can aggregate data from other views. Without the use of views it would be much harder to normalise databases above second normal form. Views can make it easier to create lossless join decomposition.

QUESTION 72
The control measures that are intended to reveal the violations of security policy using software and hardware are associated with:

A. Preventive/physical
B. Detective/technical
C. Detective/physical
D. Detective/administrative

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The detective/technical control measures are intended to reveal the violations of security policy using technical means.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 35.

QUESTION 73
The controls that usually require a human to evaluate the input from sensors or cameras to determine if a real threat exists are associated with:

A. Preventive/physical
B. Detective/technical
C. Detective/physical
D. Detective/administrative

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Detective/physical controls usually require a human to evaluate the input from sensors or cameras to determine if a real threat exists. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep

Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36.

QUESTION 74
A central authority determines what subjects can have access to certain objects based on the organizational security policy is called:

A. Mandatory Access Control
B. Discretionary Access Control
C. Non-Discretionary Access Control
D. Rule-based Access control

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: A central authority determines what subjects can have access to certain objects based on the organizational security policy.
The key focal point of this question is the 'central authority' that determines access rights. Cecilia one of the quiz user has sent me feedback informing me that NIST defines MAC as: "MAC Policy means that Access Control Policy Decisions are made by a CENTRAL AUTHORITY. Which seems to indicate there could be two good answers to this question. However if you read the NISTR document mentioned in the references below, it is also mentioned that: MAC is the most mentioned NDAC policy. So MAC is a form of NDAC policy. Within the same document it is also mentioned: "In general, all access control policies other than DAC are grouped in the category of non- discretionary access control (NDAC). As the name implies, policies in this category have rules that are not established at the discretion of the user. Non-discretionary policies establish controls that cannot be changed by users, but only through administrative action."
Under NDAC you have two choices:
Rule Based Access control and Role Base Access Control MAC is implemented using RULES which makes it fall under RBAC which is a form of NDAC. It is a subset of NDAC.
This question is representative of what you can expect on the real exam where you have more than once choice that seems to be right. However, you have to look closely if one of the choices would be higher level or if one of the choice falls under one of the other choice. In this case NDAC is a better choice because MAC is falling under NDAC through the use of Rule Based Access Control.
The following are incorrect answers:
MANDATORY ACCESS CONTROL
In Mandatory Access Control the labels of the object and the clearance of the subject determines access rights, not a central authority. Although a central authority (Better known as the Data Owner) assigns the label to the object, the system does the determination of access rights automatically by comparing the Object label with the Subject clearance. The subject clearance MUST dominate (be equal or higher) than the object being accessed. The need for a MAC mechanism arises when the security policy of a system dictates that:
1. Protection decisions must not be decided by the object owner.
2. The system must enforce the protection decisions (i.e., the system enforces the security policy over the wishes or intentions of the object owner).
Usually a labeling mechanism and a set of interfaces are used to determine access based on the MAC policy; for example, a user who is running a process at the Secret classification should not be allowed to read a file with a label of Top Secret. This is known as the "simple security rule," or "no read up."
Conversely, a user who is running a process with a label of Secret should not be allowed to write to a file with a label of Confidential. This rule is called the "*-property" (pronounced "star property") or "no write down." The *-property is required to maintain system security in an automated environment.
DISCRETIONARY ACCESS CONTROL
In Discretionary Access Control the rights are determined by many different entities, each of the persons who have created files and they are the owner of that file, not one central authority. DAC leaves a certain amount of access control to the discretion of the object's owner or anyone else who is authorized to control the object's access. For example, it is generally used to limit a user's access to a file; it is the owner of the file who controls other users' accesses to the file. Only those users specified by the owner may have some combination of read, write, execute, and other permissions to the file.
DAC policy tends to be very flexible and is widely used in the commercial and government sectors. However, DAC is known to be inherently weak for two reasons:

First, granting read access is transitive; for example, when Ann grants Bob read access to a file, nothing stops Bob from copying the contents of Ann's file to an object that Bob controls. Bob may now grant any other user access to the copy of Ann's file without Ann's knowledge. Second, DAC policy is vulnerable to Trojan horse attacks. Because programs inherit the identity of the invoking user, Bob may, for example, write a program for Ann that, on the surface, performs some useful function, while at the same time destroys the contents of Ann's files. When investigating the problem, the audit files would indicate that Ann destroyed her own files. Thus, formally, the drawbacks of DAC are as follows:

Discretionary Access Control (DAC) Information can be copied from one object to another; therefore, there is no real assurance on the flow of information in a system. No restrictions apply to the usage of information when the user has received it. The privileges for accessing objects are decided by the owner of the object, rather than through a system-wide policy that reflects the organization's security requirements. ACLs and owner/group/other access control mechanisms are by far the most common mechanism for implementing DAC policies. Other mechanisms, even though not designed with DAC in mind, may have the capabilities to implement a DAC policy.

RULE BASED ACCESS CONTROL

In Rule-based Access Control a central authority could in fact determine what subjects can have access when assigning the rules for access. However, the rules actually determine the access and so this is not the most correct answer.

RuBAC (as opposed to RBAC, role-based access control) allow users to access systems and information based on pre determined and configured rules. It is important to note that there is no commonly understood definition or formally defined standard for rule-based access control as there is for DAC, MAC, and RBAC. "Rule-based access" is a generic term applied to systems that allow some form of organization-defined rules, and therefore rule-based access control encompasses a broad range of systems. RuBAC may in fact be combined with other models, particularly RBAC or DAC. A RuBAC system intercepts every access request and compares the rules with the rights of the user to make an access decision. Most of the rule-based access control relies on a security label system, which dynamically composes a set of rules defined by a security policy. Security labels are attached to all objects, including files, directories, and devices. Sometime roles to subjects (based on their attributes) are assigned as well. RuBAC meets the business needs as well as the technical needs of controlling service access. It allows business rules to be applied to access control--for example, customers who have overdue balances may be denied service access. As a mechanism for MAC, rules of RuBAC cannot be changed by users. The rules can be established by any attributes of a system related to the users such as domain, host, protocol, network, or IP addresses. For example, suppose that a user wants to access an object in another network on the other side of a router. The router employs RuBAC with the rule composed by the network addresses, domain, and protocol to decide whether or not the user can be granted access. If employees change their roles within the organization, their existing authentication credentials remain in effect and do not need to be CK configured. Using rules in conjunction with roles adds greater flexibility because rules can be applied to people as well as to devices. Rule-based access control can be combined with role-based access control, such that the role of a user is one of the attributes in rule setting. Some provisions of access control systems have rule- based policy engines in addition to a role-based policy engine and certain implemented dynamic policies [Des03]. For example, suppose that two of the primary types of software users are product engineers and quality engineers. Both groups usually have access to the same data, but they have different roles to perform in relation to the data and the application's function. In addition, individuals within each group have different job responsibilities that may be identified using several types of attributes such as developing programs and testing areas. Thus, the access decisions can be made in real time by a scripted policy that regulates the access between the groups of product engineers and quality engineers, and each individual within these groups. Rules can either replace or complement role-based access control. However, the creation of rules and security policies is also a complex process, so each organization will need to strike the appropriate balance.

References used for this question:

http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf and

AIO v3 p162-167 and OIG (2007) p.186-191

also

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

QUESTION 75

What is called the act of a user professing an identity to a system, usually in the form of a log-on ID?

A. Authentication

B. Identification
C. Authorization
D. Confidentiality

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Identification is the act of a user professing an identity to a system, usually in the form of a log-on ID to the system.
Identification is nothing more than claiming you are somebody. You identify yourself when you speak to someone on the phone that you don't know, and they ask you who they're speaking to. When you say, "I'm Jason.", you've just identified yourself. In the information security world, this is analogous to entering a username. It's not analogous to entering a password. Entering a password is a method for verifying that you are who you identified yourself as.
NOTE: The word "professing" used above means: "to say that you are, do, or feel something when other people doubt what you say". This is exactly what happen when you provide your identifier (identification), you claim to be someone but the system cannot take your word for it, you must further Authenticate to the system to prove who you claim to be.
The following are incorrect answers:
Authentication: is how one proves that they are who they say they are. When you claim to be Jane Smith by logging into a computer system as "jsmith", it's most likely going to ask you for a password. You've claimed to be that person by entering the name into the username field (that's the identification part), but now you have to prove that you are really that person. Many systems use a password for this, which is based on "something you know", i.e. a secret between you and the system.
Another form of authentication is presenting something you have, such as a driver's license, an RSA token, or a smart card.
You can also authenticate via something you are. This is the foundation for biometrics. When you do this, you first identify yourself and then submit a thumb print, a retina scan, or another form of bio-based authentication.
Once you've successfully authenticated, you have now done two things: you've claimed to be someone, and you've proven that you are that person. The only thing that's left is for the system to determine what you're allowed to do.
Authorization: is what takes place after a person has been both identified and authenticated; it's the step determines what a person can then do on the system. An example in people terms would be someone knocking on your door at night. You say, "Who is it?", and wait for a response. They say, "It's John." in order to identify themselves. You ask them to back up into the light so you can see them through the peephole. They do so, and you authenticate them based on what they look like (biometric). At that point you decide they can come inside the house.
If they had said they were someone you didn't want in your house (identification), and you then verified that it was that person (authentication), the authorization phase would not include access to the inside of the house.
Confidentiality: Is one part of the CIA triad. It prevents sensitive information from reaching the wrong people, while making sure that the right people can in fact get it. A good example is a credit card number while shopping online, the merchant needs it to clear the transaction but you do not want your informaiton exposed over the network, you would use a secure link such as SSL, TLS, or some tunneling tool to protect the information from prying eyes between point A and point B. Data encryption is a common method of ensuring confidentiality.
The other parts of the CIA triad are listed below:
Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people (for example, in a breach of confidentiality). In addition, some means must be in place to detect any changes in data that might occur as a result of non-humancaused events such as an electromagnetic pulse (EMP) or server crash. If an unexpected change occurs, a backup copy must be available to restore the affected data to its correct state. Availability is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed, providing a certain measure of redundancy and failover, providing adequate communications bandwidth and preventing the occurrence of bottlenecks, implementing emergency backup power systems, keeping current with all necessary system upgrades, and guarding against malicious actions such as denial-of-service (DoS) attacks.
Reference used for this question:

http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA http://www.danielmiessler.com/blog/security-identification-authentication-and-authorization http://www.merriam-webster.com/dictionary/profess
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36.

QUESTION 76
What is called the verification that the user's claimed identity is valid and is usually implemented through a user password at log-on time?

A. Authentication
B. Identification
C. Integrity
D. Confidentiality

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Authentication is verification that the user's claimed identity is valid and is usually implemented through a user password at log-on time.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36.

QUESTION 77
Which one of the following factors is NOT one on which Authentication is based?

A. Type 1. Something you know, such as a PIN or password
B. Type 2. Something you have, such as an ATM card or smart card
C. Type 3. Something you are (based upon one or more intrinsic physical or behavioral traits), such as a fingerprint or retina scan
D. Type 4. Something you are, such as a system administrator or security administrator

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Authentication is based on the following three factor types:
Type 1. Something you know, such as a PIN or password
Type 2. Something you have, such as an ATM card or smart card Type 3. Something you are (Unique physical characteristic), such as a fingerprint or retina scan Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36. Also: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 4: Access Control (pages 132-133).

QUESTION 78
Which type of password provides maximum security because a new password is required for each new log-on?

A. One-time or dynamic password
B. Congnitive password
C. Static password
D. Passphrase

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: "one-time password" provides maximum security because a new password is required for each new log-on.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36.

QUESTION 79
What is called a password that is the same for each log-on session?

A. "one-time password"
B. "two-time password"
C. static password
D. dynamic password

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36.

QUESTION 80
What is called a sequence of characters that is usually longer than the allotted number for a password?

A. passphrase
B. cognitive phrase
C. anticipated phrase
D. Real phrase

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: A passphrase is a sequence of characters that is usually longer than the allotted number for a password.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, page 37.

QUESTION 81
Which of the following would be true about Static password tokens?

A. The owner identity is authenticated by the token
B. The owner will never be authenticated by the token.
C. The owner will authenticate himself to the system.
D. The token does not authenticates the token owner but the system.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Password Tokens
Tokens are electronic devices or cards that supply a user's password for them. A token system can be used to supply either a static or a dynamic password. There is a big difference between the static and dynamic systems, a static system will normally log a user in but a dynamic system the user will often have to log themselves in.

Static Password Tokens:
The owner identity is authenticated by the token. This is done by the person who issues the token to the owner (normally the employer). The owner of the token is now authenticated by "something you have". The token authenticates the identity of the owner to the information system. An example of this occurring is when an employee swipes his or her smart card over an electronic lock to gain access to a store room.
Synchronous Dynamic Password Tokens:
This system is a lot more complex then the static token password. The synchronous dynamic password tokens generate new passwords at certain time intervals that are synched with the main system. The password is generated on a small device similar to a pager or a calculator that can often be attached to the user's key ring. Each password is only valid for a certain time period, typing in the wrong password in the wrong time period will invalidate the authentication. The time factor can also be the systems downfall. If a clock on the system or the password token device becomes out of synch, a user can have troubles authenticating themselves to the system.
Asynchronous Dynamic Password Tokens:
The clock synching problem is eliminated with asynchronous dynamic password tokens. This system works on the same principal as the synchronous one but it does not have a time frame. A lot of big companies use this system especially for employee's who may work from home on the companies VPN (Virtual private Network).
Challenge Response Tokens:
This is an interesting system. A user will be sent special "challenge" strings at either random or timed intervals. The user inputs this challenge string into their token device and the device will respond by generating a challenge response. The user then types this response into the system and if it is correct they are authenticated.
Reference(s) used for this question:
http://www.informit.com/guides/content.aspx?g=security&seqNum=146 and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37.

QUESTION 82
In Synchronous dynamic password tokens:

A. The token generates a new password value at fixed time intervals (this password could be based on the time of day encrypted with a secret key).

B. The token generates a new non-unique password value at fixed time intervals (this password could be based on the time of day encrypted with a secret key).

C. The unique password is not entered into a system or workstation along with an owner's PIN.

D. The authentication entity in a system or workstation knows an owner's secret key and PIN, and the entity verifies that the entered password is invalid and that it was entered during the invalid time window.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Synchronous dynamic password tokens:
- The token generates a new password value at fixed time intervals (this password could be the time of day encrypted with a secret key).
- the unique password is entered into a system or workstation along with an owner's PIN.
- The authentication entity in a system or workstation knows an owner's secret key and PIN, and the entity verifies that the entered password is valid and that it was entered during the valid time window.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37.

QUESTION 83
Which of the following choices describe a Challenge-response tokens generation?

A. A workstation or system that generates a random challenge string that the user enters into the token when prompted along with the proper PIN.

B. A workstation or system that generates a random login id that the user enters when prompted along with the proper PIN.

C. A special hardware device that is used to generate ramdom text in a cryptography system.

D. The authentication mechanism in the workstation or system does not determine if the owner should be authenticated.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Challenge-response tokens are:
- A workstation or system generates a random challenge string and the owner enters the string into the token along with the proper PIN.
- The token generates a response that is then entered into the workstation or system.
- The authentication mechanism in the workstation or system then determines if the owner should be authenticated.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37. Also: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 4: Access Control (pages 136-137).

QUESTION 84
What is called an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics?

A. Biometrics

B. Micrometrics

C. Macrometrics

D. MicroBiometrics

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The
Answer: Biometrics; Biometrics are defined as an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 37,38.

QUESTION 85
In biometrics, "one-to-many" search against database of stored biometric images is done in:

A. Authentication

B. Identification

C. Identities

D. Identity-based access control

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: In biometrics, identification is a "one-to-many" search of an individual's characteristics from a database of stored images.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 38.

QUESTION 86
In biometrics, the "one-to-one" search used to verify claim to an identity made by a person is considered:

A. Authentication
B. Identification
C. Auditing
D. Authorization

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Biometric devices can be use for either IDENTIFICATION or AUTHENTICATION ONE TO ONE is for AUTHENTICATION
This means that you as a user would provide some biometric credential such as your fingerprint. Then they will compare the template that you have provided with the one stored in the Database. If the two are exactly the same that prove that you are who you pretend to be.
ONE TO MANY is for IDENTIFICATION
A good example of this would be within airport. Many airports today have facial recognition cameras, as you walk through the airport it will take a picture of your face and then compare the template (your face) with a database full of templates and see if there is a match between your template and the ones stored in the Database. This is for IDENTIFICATION of a person. Some additional clarification or comments that might be helpful are: Biometrics establish authentication using specific information and comparing results to expected data. It does not perform well for identification purposes such as scanning for a person's face in a moving crowd for example.
Identification methods could include: username, user ID, account number, PIN, certificate, token, smart card, biometric device or badge.
Auditing is a process of logging or tracking what was done after the identity and authentication process is completed.
Authorization is the rights the subject is given and is performed after the identity is established.
Reference OIG (2007) p148, 167
Authentication in biometrics is a "one-to-one" search to verify claim to an identity made by a person.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 38.

QUESTION 87
What is called the percentage of valid subjects that are falsely rejected by a Biometric Authentication system?

A. False Rejection Rate (FRR) or Type I Error
B. False Acceptance Rate (FAR) or Type II Error
C. Crossover Error Rate (CER)
D. True Rejection Rate (TRR) or Type III Error

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The percentage of valid subjects that are falsely rejected is called the False Rejection Rate (FRR) or Type I Error.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 38.

QUESTION 88
What is called the percentage at which the False Rejection Rate equals the False Acceptance Rate?

A. False Rejection Rate (FRR) or Type I Error
B. False Acceptance Rate (FAR) or Type II Error
C. Crossover Error Rate (CER)

D. Failure to enroll rate (FTE or FER)

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The percentage at which the False Rejection Rate equals the False Acceptance Rate is called the Crossover Error Rate (CER). Another name for the CER is the Equal Error Rate (EER), any of the two terms could be used.
Equal error rate or crossover error rate (EER or CER)
It is the rate at which both accept and reject errors are equal. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is most accurate.
The other choices were all wrong answers:
The following are used as performance metrics for biometric systems:
false accept rate or false match rate (FAR or FMR): the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted. This is when an impostor would be accepted by the system.
False reject rate or false non-match rate (FRR or FNMR): the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected. This is when a valid company employee would be rejected by the system.
Failure to enroll rate (FTE or FER): the rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low quality inputs.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 38.
and
https://en.wikipedia.org/wiki/Biometrics

QUESTION 89
Considerations of privacy, invasiveness, and psychological and physical comfort when using the system are important elements for which of the following?

A. Accountability of biometrics systems
B. Acceptability of biometrics systems
C. Availability of biometrics systems
D. Adaptability of biometrics systems

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Acceptability refers to considerations of privacy, invasiveness, and psychological and physical comfort when using the system.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 39.

QUESTION 90
Which of the following biometric characteristics cannot be used to uniquely authenticate an individual's identity?

A. Retina scans
B. Iris scans
C. Palm scans
D. Skin scans

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The following are typical biometric characteristics that are used to uniquely authenticate an individual's identity:
Fingerprints
Retina scans
Iris scans
Facial scans
Palm scans
Hand geometry
Voice
Handwritten signature dynamics
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 39. And: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 4: Access Control (pages 127-131).

QUESTION 91
Which of the following offers advantages such as the ability to use stronger passwords, easier password administration, one set of credential, and faster resource access?

A. Smart cards
B. Single Sign-On (SSO)
C. Symmetric Ciphers
D. Public Key Infrastructure (PKI)

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The advantages of SSO include having the ability to use stronger passwords, easier administration as far as changing or deleting the passwords, minimize the risks of orphan accounts, and requiring less time to access resources. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 39.

QUESTION 92
Which of the following describes the major disadvantage of many Single Sign-On (SSO) implementations?

A. Once an individual obtains access to the system through the initial log-on, they have access to all resources within the environment that the account has access to.
B. The initial logon process is cumbersome to discourage potential intruders.
C. Once a user obtains access to the system through the initial log-on, they only need to logon to some applications.
D. Once a user obtains access to the system through the initial log-on, he has to logout from all other systems

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Single Sign-On is a distrubuted Access Control methodology where an individual only has to authenticate once and would have access to all primary and secondary network domains. The individual would not be required to re-authenticate when they needed additional resources. The security issue that this creates is if a fraudster is able to compromise those credential they too would have access to all the resources that account has access to. All the other answers are incorrect as they are distractors.

QUESTION 93
Which of the following is implemented through scripts or smart agents that replays the users multiple log-ins against authentication servers to verify a user's identity which permit access to system services?

A. Single Sign-On
B. Dynamic Sign-On
C. Smart cards
D. Kerberos

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: SSO can be implemented by using scripts that replay the users multiple log-ins against authentication servers to verify a user's identity and to permit access to system services. Single Sign on was the best answer in this case because it would include Kerberos. When you have two good answers within the 4 choices presented you must select the BEST one. The high level choice is always the best. When one choice would include the other one that would be the best as well.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 40.

QUESTION 94
Which of the following is a trusted, third party authentication protocol that was developed under Project Athena at MIT?

A. Kerberos
B. SESAME
C. KryptoKnight
D. NetSP

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Kerberos is a trusted, third party authentication protocol that was developed under Project Athena at MIT.
Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. A free implementation of this protocol is available from the Massachusetts Institute of Technology. Kerberos is available in many commercial products as well.
The Internet is an insecure place. Many of the protocols used in the Internet do not provide any security. Tools to "sniff" passwords off of the network are in common use by systems crackers. Thus, applications which send an unencrypted password over the network are extremely vulnerable. Worse yet, other client/server applications rely on the client program to be "honest" about the identity of the user who is using it. Other applications rely on the client to restrict its activities to those which it is allowed to do, with no other enforcement by the server. Some sites attempt to use firewalls to solve their network security problems. Unfortunately, firewalls assume that "the bad guys" are on the outside, which is often a very bad assumption. Most of the really damaging incidents of computer crime are carried out by insiders. Firewalls also have a significant disadvantage in that they restrict how your users can use the Internet. (After all, firewalls are simply a less extreme example of the dictum that there is nothing more secure then a computer which is not connected to the network --- and powered off!) In many places, these restrictions are simply unrealistic and unacceptable.
Kerberos was created by MIT as a solution to these network security problems. The Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection. After a client and server have used Kerberos to prove their identity, they can also encrypt all of their communications to assure privacy and data integrity as they go about their business.
Kerberos is freely available from MIT, under a copyright permission notice very similar to the one used for the BSD operating and X11 Windowing system. MIT provides Kerberos in source form, so that anyone who wishes to use it may look over the code for themselves and assure themselves that the code is trustworthy. In addition, for those who prefer to rely on a professional supported product, Kerberos is available as a product

from many different vendors. In summary, Kerberos is a solution to your network security problems. It provides the tools of authentication and strong cryptography over the network to help you secure your information systems across your entire enterprise. We hope you find Kerberos as useful as it has been to us. At MIT, Kerberos has been invaluable to our Information/Technology architecture. KryptoKnight is a Peer to Peer authentication protocol incorporated into the NetSP product from IBM.
SESAME is an authentication and access control protocol, that also supports communication confidentiality and integrity. It provides public key based authentication along with the Kerberos style authentication, that uses symmetric key cryptography. Sesame supports the Kerberos protocol and adds some security extensions like public key based authentication and an ECMAstyle Privilege Attribute Service. The complete Sesame protocol is a two step process. In the first step, the client successfully authenticates itself to the Authentication Server and obtains a ticket that can be presented to the Privilege Attribute Server. In the second step, the initiator obtains proof of his access rights in the form of Privilege Attributes Certificate (PAC). The PAC is a specific form of Access Control Certificate as defined in the ECMA-219 document. This document describes the extensions to Kerberos for public key based authentication as adopted in Sesame. SESAME, KryptoKnight, and NetSP never took off and the protocols are no longer commonly used.

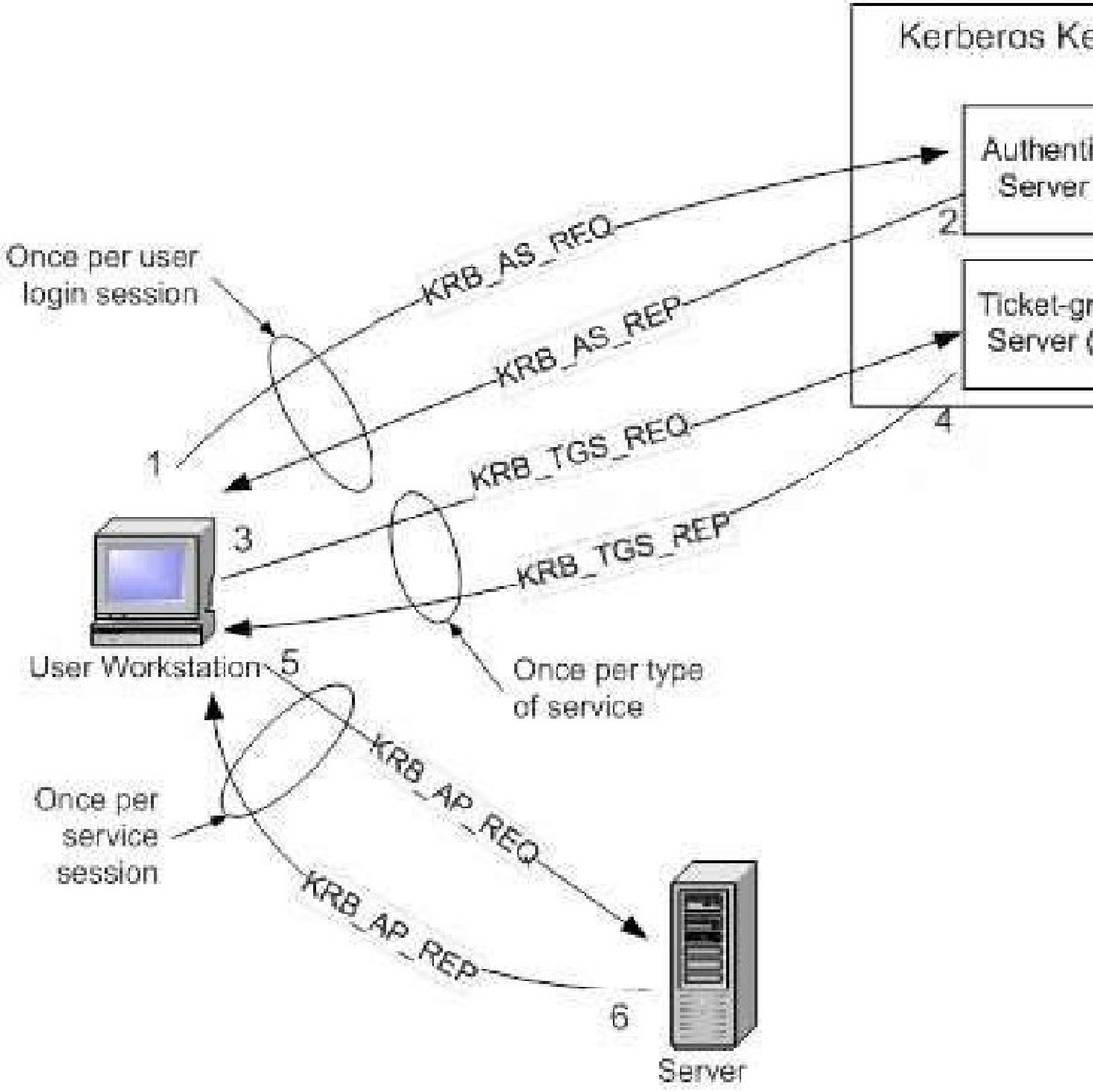
http://www.cmf.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html#whatis and
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 40.

QUESTION 95
Which of the following is NOT true of the Kerberos protocol?

A. Only a single login is required per session.
B. The initial authentication steps are done using public key algorithm.
C. The KDC is aware of all systems in the network and is trusted by all of them
D. It performs mutual authentication

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. It has the following characteristics:
It is secure: it never sends a password unless it is encrypted. Only a single login is required per session. Credentials defined at login are then passed between resources without the need for additional logins.
The concept depends on a trusted third party a Key Distribution Center (KDC). The KDC is aware of all systems in the network and is trusted by all of them. It performs mutual authentication, where a client proves its identity to a server and a server proves its identity to the client.
Kerberos introduces the concept of a Ticket-Granting Server/Service (TGS). A client that wishes to use a service has to receive a ticket from the TGS a ticket is a time-limited cryptographic message giving it access to the server. Kerberos also requires an Authentication Server (AS) to verify clients. The two servers combined make up a KDC. Within the Windows environment, Active Directory performs the functions of the KDC. The following figure shows the sequence of events required for a client to gain access to a service using Kerberos authentication. Each step is shown with the Kerberos message associated with it, as defined in RFC 4120 "The Kerberos Network Authorization Service (V5)".



Kerberos Authentication Step by Step

Step 1: The user logs on to the workstation and requests service on the host. The workstation sends a message to the Authorization Server requesting a ticket granting ticket (TGT). Step 2: The Authorization Server verifies the user's access rights in the user database and creates a TGT and session key. The Authorization Sever encrypts the results using a key derived from the user's password and sends a message back to the user workstation. The workstation prompts the user for a password and uses the password to decrypt the incoming message. When decryption succeeds, the user will be able to use the TGT to request a service ticket.

Step 3: When the user wants access to a service, the workstation client application sends a request to the

Ticket Granting Service containing the client name, realm name and a timestamp. The user proves his identity by sending an authenticator encrypted with the session key received in Step 2.
Step 4: The TGS decrypts the ticket and authenticator, verifies the request, and creates a ticket for the requested server. The ticket contains the client name and optionally the client IP address. It also contains the realm name and ticket lifespan. The TGS returns the ticket to the user workstation. The returned message contains two copies of a server session key one encrypted with the client password, and one encrypted by the service password. Step 5: The client application now sends a service request to the server containing the ticket received in Step 4 and an authenticator. The service authenticates the request by decrypting the session key. The server verifies that the ticket and authenticator match, and then grants access to the service. This step as described does not include the authorization performed by the Intel AMT device, as described later.
Step 6: If mutual authentication is required, then the server will reply with a server authentication message.
The Kerberos server knows "secrets" (encrypted passwords) for all clients and servers under its control, or it is in contact with other secure servers that have this information. These "secrets" are used to encrypt all of the messages shown in the figure above. To prevent "replay attacks," Kerberos uses timestamps as part of its protocol definition. For timestamps to work properly, the clocks of the client and the server need to be in synch as much as possible. In other words, both computers need to be set to the same time and date. Since the clocks of two computers are often out of synch, administrators can establish a policy to establish the maximum acceptable difference to Kerberos between a client's clock and server's clock. If the difference between a client's clock and the server's clock is less than the maximum time difference specified in this policy, any timestamp used in a session between the two computers will be considered authentic. The maximum difference is usually set to five minutes. Note that if a client application wishes to use a service that is "Kerberized" (the service is configured to perform Kerberos authentication), the client must also be Kerberized so that it expects to support the necessary message responses.
For more information about Kerberos, see http://web.mit.edu/kerberos/www/.

Introduction to Kerberos Authentication from Intel
and
http://www.zeroshell.net/eng/kerberos/Kerberos-definitions/#1.3.5.3 and
http://www.ietf.org/rfc/rfc4120.txt

QUESTION 96
Which of the following is addressed by Kerberos?

A. Confidentiality and Integrity
B. Authentication and Availability
C. Validation and Integrity
D. Auditability and Integrity

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Kerberos addresses the confidentiality and integrity of information. It also addresses primarily authentication but does not directly address availability.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 42.
and
https://www.ietf.org/rfc/rfc4120.txt
and
http://learn-networking.com/network-security/how-kerberos-authentication-works

QUESTION 97
Kerberos is vulnerable to replay in which of the following circumstances?

A. When a private key is compromised within an allotted time window.
B. When a public key is compromised within an allotted time window.

C. When a ticket is compromised within an allotted time window.

D. When the KSD is compromised within an allotted time window.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Replay can be accomplished on Kerberos if the compromised tickets are used within an allotted time window.
The security depends on careful implementation:enforcing limited lifetimes for authentication credentials minimizes the threat of of replayed credentials, the KDC must be physically secured, and it should be hardened, not permitting any non-kerberos activities. Official ISC2 Guide to the CISSP, 2007 Edition, page 184 also see:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 42.

QUESTION 98
Like the Kerberos protocol, SESAME is also subject to which of the following?

A. timeslot replay

B. password guessing

C. symmetric key guessing

D. asymmetric key guessing

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Sesame is an authentication and access control protocol, that also supports communication confidentiality and integrity. It provides public key based authentication along with the Kerberos style authentication, that uses symmetric key cryptography. Sesame supports the Kerberos protocol and adds some security extensions like public key based authentication and an ECMA-style Privilege Attribute Service.
The users under SESAME can authenticate using either symmetric encryption as in Kerberos or Public Key authentication. When using Symmetric Key authentication as in Kerberos, SESAME is also vulnerable to password guessing just like Kerberos would be. The Symmetric key being used is based on the password used by the user when he logged on the system. If the user has a simple password it could be guessed or compromise. Even thou Kerberos or SESAME may be use, there is still a need to have strong password discipline. The Basic Mechanism in Sesame for strong authentication is as follow:
The user sends a request for authentication to the Authentication Server as in Kerberos, except that SESAME is making use of public key cryptography for authentication where the client will present his digital certificate and the request will be signed using a digital signature. The signature is communicated to the authentication server through the preauthentication fields. Upon receipt of this request, the authentication server will verifies the certificate, then validate the signature, and if all is fine the AS will issue a ticket granting ticket (TGT) as in Kerberos. This TGT will be use to communicate with the privilage attribute server (PAS) when access to a resource is needed. Users may authenticate using either a public key pair or a conventional (symmetric) key. If public key cryptography is used, public key data is transported in preauthentication data fields to help establish identity.
Kerberos uses tickets for authenticating subjects to objects and SESAME uses Privileged Attribute Certificates (PAC), which contain the subject's identity, access capabilities for the object, access time period, and lifetime of the PAC. The PAC is digitally signed so that the object can validate that it came from the trusted authentication server, which is referred to as the privilege attribute server (PAS). The PAS holds a similar role as the KDC within Kerberos. After a user successfully authenticates to the authentication service (AS), he is presented with a token to give to the PAS. The PAS then creates a PAC for the user to present to the resource he is trying to access.
Reference(s) used for this question:
http://srg.cs.uiuc.edu/Security/nephilim/Internal/SESAME.txt and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 43.

QUESTION 99
RADIUS incorporates which of the following services?

A. Authentication server and PIN codes.
B. Authentication of clients and static passwords generation.
C. Authentication of clients and dynamic passwords generation.
D. Authentication server as well as support for Static and Dynamic passwords.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: A Network Access Server (NAS) operates as a client of RADIUS. The client is responsible for passing user information to
designated RADIUS servers, and then acting on the response which is returned. RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user. RADIUS authentication is based on provisions of simple username/password credentials. These credentials are encrypted
by the client using a shared secret between the client and the RADIUS server. OIG 2007, Page RADIUS incorporates an authentication server and can make uses of both dynamic and static passwords.
Since it uses the PAP and CHAP protocols, it also incluses static passwords. RADIUS is an Internet protocol. RADIUS carries authentication, authorization, and configuration information between a Network Access Server and a shared Authentication Server. RADIUS features and functions are described primarily in the IETF (International Engineering Task Force) document RFC2138.
The term " RADIUS" is an acronym which stands for Remote Authentication Dial In User Service. The main advantage to using a RADIUS approach to authentication is that it can provide a stronger form of authentication. RADIUS is capable of using a strong, two-factor form of authentication, in which users need to possess both a user ID and a hardware or software token to gain access.
Token-based schemes use dynamic passwords. Every minute or so, the token generates a unique 4-, 6- or 8-digit access number that is synchronized with the security server. To gain entry into the system, the user must generate both this one-time number and provide his or her user ID and password.
Although protocols such as RADIUS cannot protect against theft of an authenticated session via some realtime attacks, such as wiretapping, using unique, unpredictable authentication requests can protect against a wide range of active attacks.
RADIUS: Key Features and Benefits
Features Benefits
RADIUS supports dynamic passwords and challenge/response passwords. Improved system security due to the fact that passwords are not static. It is much more difficult for a bogus host to spoof users into giving up their passwords or password-generation algorithms.
RADIUS allows the user to have a single user ID and password for all computers in a network. Improved usability due to the fact that the user has to remember only one login combination.
RADIUS is able to:
Prevent RADIUS users from logging in via login (or ftp).
Require them to log in via login (or ftp)
Require them to login to a specific network access server (NAS); Control access by time of day.
Provides very granular control over the types of logins allowed, on a per-user basis. The time-out interval for failing over from an unresponsive primary RADIUS server to a backup RADIUS server is site-configurable.
RADIUS gives System Administrator more flexibility in managing which users can login from which hosts or devices.
Stratus Technology Product Brief
http://www.stratus.com/products/vos/openvos/radius.htm Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 43, 44. Also check: MILLER, Lawrence & GREGORY, Peter, CISSP for Dummies, 2002, Wiley Publishing, Inc., pages 45-46.

QUESTION 100
Which of the following protects a password from eavesdroppers and supports the encryption of

communication?

A. Challenge Handshake Authentication Protocol (CHAP)
B. Challenge Handshake Identification Protocol (CHIP)
C. Challenge Handshake Encryption Protocol (CHEP)
D. Challenge Handshake Substitution Protocol (CHSP)

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: CHAP: A protocol that uses a three way hanbdshake The server sends the client a challenge which includes a random value(a nonce) to thwart replay attacks. The client responds with the MD5 hash of the nonce and the password.
The authentication is successful if the client's response is the one that the server expected.
Page 450, OIG 2007.
CHAP protects the password from eavesdroppers and supports the encryption of communication. KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 44.

QUESTION 101
The Terminal Access Controller Access Control System (TACACS) employs which of the following?

A. a user ID and static password for network access
B. a user ID and dynamic password for network access
C. a user ID and symmetric password for network access
D. a user ID and asymmetric password for network access

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: For networked applications, the Terminal Access Controller Access Control System (TACACS) employs a user ID and a static password for network access. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 44.

QUESTION 102
Which of the following is most relevant to determining the maximum effective cost of access control?

A. the value of information that is protected
B. management's perceptions regarding data importance
C. budget planning related to base versus incremental spending.
D. the cost to replace lost data

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The cost of access control must be commensurate with the value of the information that is being protected.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 49.

QUESTION 103
Which of the following is NOT a factor related to Access Control?

A. integrity
B. authenticity
C. confidentiality
D. availability

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: These factors cover the integrity, confidentiality, and availability components of information system security.
Integrity is important in access control as it relates to ensuring only authorized subjects can make changes to objects.
Authenticity is different from authentication. Authenticity pertains to something being authentic, not necessarily having a direct correlation to access control. Confidentiality is pertinent to access control in that the access to sensitive information is controlled to protect confidentiality.
vailability is protected by access controls in that if an attacket attempts to disrupt availability they would first need access.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 49.

QUESTION 104
Which of the following is most appropriate to notify an external user that session monitoring is being conducted?

A. Logon Banners
B. Wall poster
C. Employee Handbook
D. Written agreement

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Banners at the log-on time should be used to notify external users of any monitoring that is being conducted. A good banner will give you a better legal stand and also makes it obvious the user was warned about who should access the system and if it is an unauthorized user then he is fully aware of trespassing.
This is a tricky question, the keyword in the question is External user. There are two possible answers based on how the question is presented, this question could either apply to internal users or ANY anonymous user.
Internal users should always have a written agreement first, then logon banners serve as a constant reminder.
Anonymous users, such as those logging into a web site, ftp server or even a mail server; their only notification system is the use of a logon banner.
References used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 50.
and
Shon Harris, CISSP All-in-one, 5th edition, pg 873

QUESTION 105
Which of the following pairings uses technology to enforce access control policies?

A. Preventive/Administrative
B. Preventive/Technical
C. Preventive/Physical
D. Detective/Administrative

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The preventive/technical pairing uses technology to enforce access control policies.
TECHNICAL CONTROLS
Technical security involves the use of safeguards incorporated in computer hardware, operations or applications software, communications hardware and software, and related devices. Technical controls are sometimes referred to as logical controls.
Preventive Technical Controls
Preventive technical controls are used to prevent unauthorized personnel or programs from gaining remote access to computing resources. Examples of these controls include:
Access control software.
Antivirus software.
Library control systems.
Passwords.
Smart cards.
Encryption.
Dial-up access control and callback systems.
Preventive Physical Controls
Preventive physical controls are employed to prevent unauthorized personnel from entering computing facilities (i.e., locations housing computing resources, supporting utilities, computer hard copy, and input data media) and to help protect against natural disasters. Examples of these controls include:
Backup files and documentation.
Fences.
Security guards.
Badge systems.
Double door systems.
Locks and keys.
Backup power.
Biometric access controls.
Site selection.
Fire extinguishers.
Preventive Administrative Controls
Preventive administrative controls are personnel-oriented techniques for controlling people's behavior to ensure the confidentiality, integrity, and availability of computing data and programs. Examples of preventive administrative controls include:
Security awareness and technical training.
Separation of duties.
Procedures for recruiting and terminating employees.
Security policies and procedures.
Supervision.
Disaster recovery, contingency, and emergency plans.
User registration for computer access.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.

QUESTION 106
Access control is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system. It does not permit management to:

A. specify what users can do
B. specify which resources they can access
C. specify how to restrain hackers
D. specify what operations they can perform on a system.

Correct Answer: C

Explanation

Explanation/Reference:
Explanation: Access control is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system. It permits management to specify what users can do, which resources they can access, and what operations they can perform on a system. Specifying HOW to restrain hackers is not directly linked to access control.
Source: DUPUIS, Clement, Access Control Systems and Methodology, Version 1, May 2002, CISSP Open Study Group Study Guide for Domain 1, Page 12.

QUESTION 107
Access Control techniques do not include which of the following choices?

A. Relevant Access Controls
B. Discretionary Access Control
C. Mandatory Access Control
D. Lattice Based Access Control

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Access Control Techniques
Discretionary Access Control
Mandatory Access Control
Lattice Based Access Control
Rule-Based Access Control
Role-Based Access Control
Source: DUPUIS, Clement, Access Control Systems and Methodology, Version 1, May 2002, CISSP Open Study Group Study Guide for Domain 1, Page 13.

QUESTION 108
Access Control techniques do not include which of the following?

A. Rule-Based Access Controls
B. Role-Based Access Control
C. Mandatory Access Control
D. Random Number Based Access Control

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Access Control Techniques
Discretionary Access Control
Mandatory Access Control
Lattice Based Access Control
Rule-Based Access Control
Role-Based Access Control
Source: DUPUIS, Clement, Access Control Systems and Methodology, Version 1, May 2002, CISSP Open Study Group Study Guide for Domain 1, Page 13.

QUESTION 109
Which of the following statements relating to the Bell-LaPadula security model is FALSE (assuming the Strong Star property is not being used) ?

A. A subject is not allowed to read up.

B. The property restriction can be escaped by temporarily downgrading a high level subject.

C. A subject is not allowed to read down.

D. It is restricted to confidentiality.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: It is not a property of Bell LaPadula model.
The other answers are incorrect because:
A subject is not allowed to read up is a property of the 'simple security rule' of Bell LaPadula model.
The property restriction can be escaped by temporarily downgrading a high level subject can be escaped by temporarily downgrading a high level subject or by identifying a set of trusted objects which are permitted to violate the property as long as it is not in the middle of an operation. It is restricted to confidentiality as it is a state machine model that enforces the confidentiality aspects of access control.
Shon Harris AIO v3 , Chapter-5 : Security Models and Architecture , Page:279-282

QUESTION 110
Which of the following logical access exposures INVOLVES CHANGING data before, or as it is entered into the computer?

A. Data diddling

B. Salami techniques

C. Trojan horses

D. Viruses

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: It involves changing data before , or as it is entered into the computer or in other words , it refers to the alteration of the existing data.
The other answers are incorrect because :
Salami techniques : A salami attack is the one in which an attacker commits several small crimes with the hope that the overall larger crime will go unnoticed. Trojan horses: A Trojan Horse is a program that is disguised as another program. Viruses:A Virus is a small application , or a string of code , that infects applications.
Shon Harris , AIO v3
Chapter - 11: Application and System Development, Page : 875-880 Chapter - 10: Law, Investigation and Ethics , Page : 758-759

QUESTION 111
When a biometric system is used, which error type deals with the possibility of GRANTING access to impostors who should be REJECTED?

A. Type I error

B. Type II error

C. Type III error

D. Crossover error

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: When the biometric system accepts impostors who should have been rejected , it is called a Type II error or False Acceptance Rate or False Accept Rate. Biometrics verifies an individual's identity by analyzing

a unique personal attribute or behavior, which is one of the most effective and accurate methods of verifying identification. Biometrics is a very sophisticated technology; thus, it is much more expensive and complex than the other types of identity verification processes. A biometric system can make authentication decisions based on an individual's behavior, as in signature dynamics, but these can change over time and possibly be forged. Biometric systems that base authentication decisions on physical attributes (iris, retina, fingerprint) provide more accuracy, because physical attributes typically don't change much, absent some disfiguring injury, and are harder to impersonate.

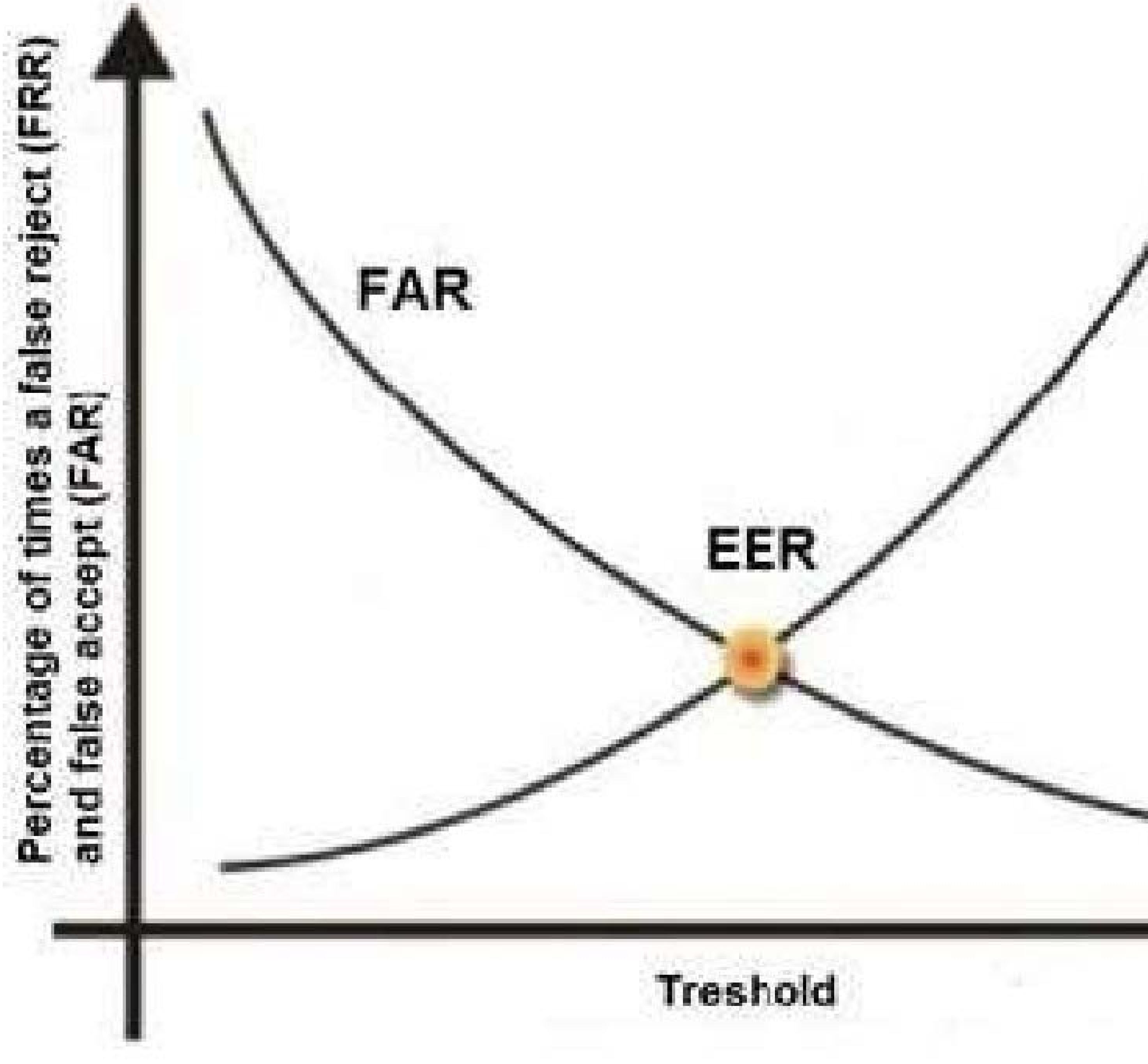
When a biometric system rejects an authorized individual, it is called a Type I error (False Rejection Rate (FRR) or False Reject Rate (FRR)).

When the system accepts impostors who should be rejected, it is called a Type II error (False Acceptance Rate (FAR) or False Accept Rate (FAR)). Type II errors are the most dangerous and thus the most important to avoid.

The goal is to obtain low numbers for each type of error, but When comparing different biometric systems, many different variables are used, but one of the most important metrics is the crossover error rate (CER).

The accuracy of any biometric method is measured in terms of Failed Acceptance Rate (FAR) and Failed Rejection Rate (FRR). Both are expressed as percentages. The FAR is the rate at which attempts by unauthorized users are incorrectly accepted as valid. The FRR is just the opposite. It measures the rate at which authorized users are denied access. The relationship between FRR (Type I) and FAR (Type II) is depicted in the graphic below . As one rate increases, the other decreases. The Cross-over Error Rate (CER) is sometimes considered a good indicator of the overall accuracy of a biometric system. This is the point at which the FRR and the FAR have the same value. Solutions with a lower CER are typically more accurate.

See graphic below from Biometria showing this relationship. The Cross-over Error Rate (CER) is also called the Equal Error Rate (EER), the two are synonymous.



Cross Over Error Rate
The other answers are incorrect:
Type I error is also called as False Rejection Rate where a valid user is rejected by the system. Type III error : there is no such error type in biometric system. Crossover error rate stated in percentage , represents the point at which false rejection equals the false acceptance rate.
Reference(s) used for this question:
http://www.biometria.sk/en/principles-of-biometrics.html and
Shon Harris, CISSP All In One (AIO), 6th Edition , Chapter 3, Access Control, Page 188-189 and
Tech Republic, Reduce Multi_Factor Authentication Cost

QUESTION 112
Which of the following is the FIRST step in protecting data's confidentiality?

A. Install a firewall
B. Implement encryption
C. Identify which information is sensitive
D. Review all user access rights

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: In order to protect the confidentiality of the data.
The following answers are incorrect because :
Install a firewall is incorrect as this would come after the information has been identified for sensitivity levels.
Implement encryption is also incorrect as this is one of the mechanisms to protect the data once it has been identified.
Review all user access rights is also incorrect as this is also a protection mechanism for the identified information.
Reference : Shon Harris AIO v3 , Chapter-4 : Access Control , Page : 126

QUESTION 113
Which of the following best ensures accountability of users for the actions taken within a system or domain?

A. Identification
B. Authentication
C. Authorization
D. Credentials

Correct Answer: B
Explanation

Explanation/Reference:
Details:
The only way to ensure accountability is if the subject is uniquely identified and authenticated. Identification alone does not provide proof the user is who they claim to be. After showing proper credentials, a user is authorized access to resources.

HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 4: Access Control (page 126).

QUESTION 114
Which of the following statements pertaining to biometrics is FALSE?

A. User can be authenticated based on behavior.
B. User can be authenticated based on unique physical attributes.
C. User can be authenticated by what he knows.
D. A biometric system's accuracy is determined by its crossover error rate (CER).

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: As this is not a characteristic of Biometrics this is the rigth choice for this question. This is one of the three basic way authentication can be performed and it is not related to Biometrics. Example of something you know would be a password or PIN for example. Please make a note of the negative 'FALSE' within the

question. This question may seem tricky to some of you but you would be amazed at how many people cannot deal with negative questions. There will be a few negative questions within the real exam, just like this one the keyword NOT or FALSE will be in Uppercase to clearly indicate that it is negative. Biometrics verifies an individual's identity by analyzing a unique personal attribute or behavior, which is one of the most effective and accurate methods of performing authentication (one to one matching) or identification (a one to many matching).
A biometric system scans an attribute or behavior of a person and compares it to a template store within an authentication server datbase, such template would be created in an earlier enrollment process. Because this system inspects the grooves of a person's fingerprint, the pattern of someone's retina, or the pitches of someone's voice, it has to be extremely sensitive. The system must perform accurate and repeatable measurements of anatomical or physiological characteristics. This type of sensitivity can easily cause false positives or false negatives. The system must be calibrated so that these false positives and false negatives occur infrequently and the results are as accurate as possible.
There are two types of failures in biometric identification:
False Rejection also called False Rejection Rate (FRR) -- The system fail to recognize a legitimate user. While it could be argued that this has the effect of keeping the protected area extra secure, it is an intolerable frustration to legitimate users who are refused access because the scanner does not recognize them.
False Acceptance or False Acceptance Rate (FAR) -- This is an erroneous recognition, either by confusing one user with another or by accepting an imposter as a legitimate user.
Physiological Examples:
Unique Physical Attributes:
Fingerprint (Most commonly accepted)
Hand Geometry
Retina Scan (Most accurate but most intrusive)
Iris Scan
Vascular Scan
Behavioral Examples:
Repeated Actions
Keystroke Dynamics
(Dwell time (the time a key is pressed) and Flight time (the time between "key up" and the next "key down").
Signature Dynamics
(Stroke and pressure points)
EXAM TIP:
Retina scan devices are the most accurate but also the most invasive biometrics system available today. The continuity of the retinal pattern throughout life and the difficulty in fooling such a device also make it a great long-term, high-security option. Unfortunately, the cost of the proprietary hardware as well the stigma of users thinking it is potentially harmful to the eye makes retinal scanning a bad fit for most situations.
Remember for the exam that fingerprints are the most commonly accepted type of biometrics system.
The other answers are incorrect:
'Users can be authenticated based on behavior.' is incorrect as this choice is TRUE as it pertains to BIOMETRICS.
Biometrics systems makes use of unique physical characteristics or behavior of users. 'User can be authenticated based on unique physical attributes.' is also incorrect as this choice is also TRUE as it pertains to BIOMETRICS. Biometrics systems makes use of unique physical characteristics or behavior of users.
'A biometric system's accuracy is determined by its crossover error rate (CER)' is also incorrect as this is TRUE as it also pertains to BIOMETRICS. The CER is the point at which the false rejection rates and the false acceptance rates are equal. The smaller the value of the CER, the more accurate the system.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 25353-25356). Auerbach Publications. Kindle Edition.
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 25297-25303). Auerbach Publications. Kindle Edition.

QUESTION 115
Which of the following biometric devices offers the LOWEST CER?

A. Keystroke dynamics

B. Voice verification

C. Iris scan

D. Fingerprint

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: From most effective (lowest CER) to least effective (highest CER) are:
Iris scan, fingerprint, voice verification, keystroke dynamics. Reference : Shon Harris Aio v3 , Chapter-4 : Access Control , Page : 131 Also see: http://www.sans.org/reading_room/whitepapers/authentication/biometric-selection-bodyparts- online_139

QUESTION 116
Which of the following is the LEAST user accepted biometric device?

A. Fingerprint

B. Iris scan

C. Retina scan

D. Voice verification

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The biometric device that is least user accepted is the retina scan, where a system scans the blood-vessel pattern on the backside of the eyeball. When using this device, an individual has to place their eye up to a device, and may require a puff of air to be blown into the eye. The iris scan only needs for an individual to glance at a camera that could be placed above a door.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 4: Access Control (page 131).

QUESTION 117
Which of the following is the WEAKEST authentication mechanism?

A. Passphrases

B. Passwords

C. One-time passwords

D. Token devices

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Most of the time users usually choose passwords which can be guessed , hence passwords is the BEST answer out of the choices listed above.
The following answers are incorrect because :
Passphrases is incorrect as it is more secure than a password because it is longer. One-time passwords is incorrect as the name states , it is good for only once and cannot be reused.
Token devices is incorrect as this is also a password generator and is an one time password mechanism.
Reference : Shon Harris AIO v3 , Chapter-4 : Access Control , Page : 139 , 142.

QUESTION 118
Which of the following statements pertaining to access control is false?

A. Users should only access data on a need-to-know basis.

B. If access is not explicitly denied, it should be implicitly allowed.

C. Access rights should be granted based on the level of trust a company has on a subject.

D. Roles can be an efficient way to assign rights to a type of user who performs certain tasks.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Access control mechanisms should default to no access to provide the necessary level of security and ensure that no security holes go unnoticed. If access is not explicitly allowed, it should be implicitly denied.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 4: Access Control (page 143).

QUESTION 119
Which of the following is NOT part of the Kerberos authentication protocol?

A. Symmetric key cryptography

B. Authentication service (AS)

C. Principals

D. Public Key

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: There is no such component within kerberos environment. Kerberos uses only symmetric encryption and does not make use of any public key component.
The other answers are incorrect because :
Symmetric key cryptography is a part of Kerberos as the KDC holds all the users' and services' secret keys.
Authentication service (AS) : KDC (Key Distribution Center) provides an authentication service Principals : Key Distribution Center provides services to principals , which can be users , applications or network services.
Shon Harris , AIO v3 , Chapter - 4: Access Control , Pages : 152-155.

QUESTION 120
Which access control model enables the OWNER of the resource to specify what subjects can access specific resources based on their identity?

A. Discretionary Access Control

B. Mandatory Access Control

C. Sensitive Access Control

D. Role-based Access Control

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Data owners decide who has access to resources based only on the identity of the person accessing the resource.
The following answers are incorrect :
Mandatory Access Control : users and data owners do not have as much freedom to determine who can access files. The operating system makes the final decision and can override the users' wishes and access decisions are based on security labels. Sensitive Access Control : There is no such access control in the context of the above question. Role-based Access Control : uses a centrally administered set of controls to determine how subjects and objects interact , also called as non discretionary access control. In a mandatory access control (MAC) model, users and data owners do not have as much freedom to determine who can access files. The operating system makes the final decision and can override the users' wishes. This model is much more structured and strict and is based on a security label system. Users are given a security clearance

(secret, top secret, confidential, and so on), and data is classified in the same way. The clearance and classification data is stored in the security labels, which are bound to the specific subjects and objects. When the system makes a decision about fulfilling a request to access an object, it is based on the clearance of the subject, the classification of the object, and the security policy of the system. The rules for how subjects access objects are made by the security officer, configured by the administrator, enforced by the operating system, and supported by security technologies Reference : Shon Harris , AIO v3 , Chapter-4 : Access Control , Page : 163-165

QUESTION 121
Which of the following access control models is based on sensitivity labels?

A. Discretionary access control
B. Mandatory access control
C. Rule-based access control
D. Role-based access control

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Access decisions are made based on the clearance of the subject and the sensitivity label of the object.
Example: Eve has a "Secret" security clearance and is able to access the "Mugwump Missile Design Profile" because its sensitivity label is "Secret." She is denied access to the "Presidential Toilet Tissue Formula" because its sensitivity label is "Top Secret." The other answers are not correct because:
Discretionary Access Control is incorrect because in DAC access to data is determined by the data owner. For example, Joe owns the "Secret Chili Recipe" and grants read access to Charles. Role Based Access Control is incorrect because in RBAC access decsions are made based on the role held by the user. For example, Jane has the role "Auditor" and that role includes read permission on the "System Audit Log."
Rule Based Access Control is incorrect because it is a form of MAC. A good example would be a Firewall where rules are defined and apply to anyone connecting through the firewall.

All in One third edition, page 164.
Official ISC2 Guide page 187.

QUESTION 122
Which access control model is also called Non Discretionary Access Control (NDAC)?

A. Lattice based access control
B. Mandatory access control
C. Role-based access control
D. Label-based access control

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: RBAC is sometimes also called non-discretionary access control (NDAC) (as Ferraiolo says "to distinguish it from the policy-based specifics of MAC"). Another model that fits within the NDAC category is Rule-Based Access Control (RuBAC or RBAC). Most of the CISSP books use the same acronym for both models but NIST tend to use a lowercase "u" in between R and B to differentiate the two models.
You can certainly mimic MAC using RBAC but true MAC makes use of Labels which contains the sensitivity of the objects and the categories they belong to. No labels means MAC is not being used.
One of the most fundamental data access control decisions an organization must make is the amount of control it will give system and data owners to specify the level of access users of that data will have. In every organization there is a balancing point between the access controls enforced by organization and system policy and the ability for information owners to determine who can have access based on specific business

requirements. The process of translating that balance into a workable access control model can be defined by three general access frameworks:

Discretionary access control

Mandatory access control

Nondiscretionary access control

A role-based access control (RBAC) model bases the access control authorizations on the roles (or functions) that the user is assigned within an organization. The determination of what roles have access to a resource can be governed by the owner of the data, as with DACs, or applied based on policy, as with MACs.

Access control decisions are based on job function, previously defined and governed by policy, and each role (job function) will have its own access capabilities. Objects associated with a role will inherit privileges assigned to that role. This is also true for groups of users, allowing administrators to simplify access control strategies by assigning users to groups and groups to roles.

There are several approaches to RBAC. As with many system controls, there are variations on how they can be applied within a computer system.

There are four basic RBAC architectures:

1. Non-RBAC: Non-RBAC is simply a user-granted access to data or an application by traditional mapping, such as with ACLs. There are no formal "roles" associated with the mappings, other than any identified by the particular user.
2. Limited RBAC: Limited RBAC is achieved when users are mapped to roles within a single application rather than through an organization-wide role structure. Users in a limited RBAC system are also able to access non-RBAC-based applications or data. For example, a user may be assigned to multiple roles within several applications and, in addition, have direct access to another application or system independent of his or her assigned role. The key attribute of limited RBAC is that the role for that user is defined within an application and not necessarily based on the user's organizational job function.
3. Hybrid RBAC: Hybrid RBAC introduces the use of a role that is applied to multiple applications or systems based on a user's specific role within the organization. That role is then applied to applications or systems that subscribe to the organization's role-based model. However, as the term "hybrid" suggests, there are instances where the subject may also be assigned to roles defined solely within specific applications, complimenting (or, perhaps, contradicting) the larger, more encompassing organizational role used by other systems.
4. Full RBAC: Full RBAC systems are controlled by roles defined by the organization's policy and access control infrastructure and then applied to applications and systems across the enterprise. The applications, systems, and associated data apply permissions based on that enterprise definition, and not one defined by a specific application or system. Be careful not to try to make MAC and DAC opposites of each other -- they are two different access control strategies with RBAC being a third strategy that was defined later to address some of the limitations of MAC and DAC.

The other answers are not correct because:

Mandatory access control is incorrect because though it is by definition not discretionary, it is not called "non-discretionary access control." MAC makes use of label to indicate the sensitivity of the object and it also makes use of categories to implement the need to know. Label-based access control is incorrect because this is not a name for a type of access control but simply a bogus detractor.

Lattice based access control is not adequate either. A lattice is a series of levels and a subject will be granted an upper and lower bound within the series of levels. These levels could be sensitivity levels or they could be confidentiality levels or they could be integrity levels.

Reference(s) used for this question:

All in One, third edition, page 165.

Ferraiolo, D., Kuhn, D. & Chandramouli, R. (2003). Role-Based Access Control, p. 18. Ferraiolo, D., Kuhn, D. (1992). Role-Based Access Controls. http://csrc.nist.gov/rbac/Role_Based_Access_Control-1992.html Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition :Access Control ((ISC) 2 Press) (Kindle Locations 1557-1584). Auerbach Publications. Kindle Edition. Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition :Access Control ((ISC)2 Press) (Kindle Locations 1474-1477). Auerbach Publications. Kindle Edition.

QUESTION 123

Which access model is most appropriate for companies with a high employee turnover?

A. Role-based access control

B. Mandatory access control

C. Lattice-based access control

D. Discretionary access control

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The underlying problem for a company with a lot of turnover is assuring that new employees are assigned the correct access permissions and that those permissions are removed when they leave the company.
Selecting the best answer requires one to think about the access control options in the context of a company with a lot of flux in the employee population. RBAC simplifies the task of assigning permissions because the permissions are assigned to roles which do not change based on who belongs to them. As employees join the company, it is simply a matter of assigning them to the appropriate roles and their permissions derive from their assigned role. They will implicitely inherit the permissions of the role or roles they have been assigned to. When they leave the company or change jobs, their role assignment is revoked/changed appropriately. Mandatory access control is incorrect. While controlling access based on the clearence level of employees and the sensitivity of obects is a better choice than some of the other incorrect answers, it is not the best choice when RBAC is an option and you are looking for the best solution for a high number of employees constantly leaving or joining the company. Lattice-based access control is incorrect. The lattice is really a mathematical concept that is used in formally modeling information flow (Bell-Lapadula, Biba, etc). In the context of the question, an abstract model of information flow is not an appropriate choice. CBK, pp. 324-325. Discretionary access control is incorrect. When an employee joins or leaves the company, the object owner must grant or revoke access for that employee on all the objects they own. Problems would also arise when the owner of an object leaves the company. The complexity of assuring that the permissions are added and removed correctly makes this the least desirable solution in this situation.
References
Alll in One, third edition page 165
RBAC is discussed on pp. 189 through 191 of the ISC(2) guide.

QUESTION 124
What can be defined as a list of subjects along with their access rights that are authorized to access a specific object?

A. A capability table
B. An access control list
C. An access control matrix
D. A role-based matrix

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: "It [ACL] specifies a list of users [subjects] who are allowed access to each object" CBK, p. 188
A capability table is incorrect. "Capability tables are used to track, manage and apply controls based on the object and rights, or capabilities of a subject. For example, a table identifies the object, specifies access rights allowed for a subject, and permits access based on the user's posession of a capability (or ticket) for the object." CBK, pp. 191-192. The distinction that makes this an incorrect choice is that access is based on posession of a capability by the subject. To put it another way, as noted in AIO3 on p. 169, "A capabiltiy table is different from an ACL because the subject is bound to the capability table, whereas the object is bound to the ACL." An access control matrix is incorrect. The access control matrix is a way of describing the rules for an access control strategy. The matrix lists the users, groups and roles down the left side and the resources and functions across the top. The cells of the matrix can either indicate that access is allowed or indicate the type of access. CBK pp 317 - 318. AIO3, p. 169 describes it as a table if subjects and objects specifying the access rights a certain subject possesses pertaining to specific objects.
In either case, the matrix is a way of analyzing the access control needed by a population of subjects to a population of objects. This access control can be applied using rules, ACL's, capability tables, etc.
A role-based matrix is incorrect. Again, a matrix of roles vs objects could be used as a tool for thinking about the access control to be applied to a set of objects. The results of the analysis could then be implemented

using RBAC.

CBK, Domain 2: Access Control.
AIO3, Chapter 4: Access Control

QUESTION 125
What is the difference between Access Control Lists (ACLs) and Capability Tables?

A. Access control lists are related/attached to a subject whereas capability tables are related/attached to an object.
B. Access control lists are related/attached to an object whereas capability tables are related/attached to a subject.
C. Capability tables are used for objects whereas access control lists are used for users.
D. They are basically the same.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Capability tables are used to track, manage and apply controls based on the object and rights, or capabilities of a subject. For example, a table identifies the object, specifies access rights allowed for a subject, and permits access based on the user's posession of a capability (or ticket) for the object. It is a row within the matrix. To put it another way, A capabiltiy table is different from an ACL because the subject is bound to the capability table, whereas the object is bound to the ACL.
CLEMENT NOTE:
If we wish to express this very simply:
Capabilities are attached to a subject and it describe what access the subject has to each of the objects on the row that matches with the subject within the matrix. It is a row within the matrix. ACL's are attached to objects, it describe who has access to the object and what type of access they have. It is a column within the matrix.
The following are incorrect answers:
"Access control lists are subject-based whereas capability tables are object-based" is incorrect. "Capability tables are used for objects whereas access control lists are used for users" is incorrect.
"They are basically the same" is incorrect.
References used for this question:
CBK, pp. 191 - 192
AIO3 p. 169

QUESTION 126
What can be defined as a table of subjects and objects indicating what actions individual subjects can take upon individual objects?

A. A capacity table
B. An access control list
C. An access control matrix
D. A capability table

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The matrix lists the users, groups and roles down the left side and the resources and functions across the top. The cells of the matrix can either indicate that access is allowed or indicate the type of access.
CBK pp 317 - 318.
AIO3, p. 169 describes it as a table if subjects and objects specifying the access rights a certain subject possesses pertaining to specific objects.
In either case, the matrix is a way of analyzing the access control needed by a population of subjects to a population of objects. This access control can be applied using rules, ACL's, capability tables, etc.

"A capacity table" is incorrect.
This answer is a trap for the unwary -- it sounds a little like "capability table" but is just there to distract you.
"An access control list" is incorrect.
"It [ACL] specifies a list of users [subjects] who are allowed access to each object" CBK, p. 188 Access control lists (ACL) could be used to implement the rules identified by an access control matrix but is different from the matrix itself.
"A capability table" is incorrect.
"Capability tables are used to track, manage and apply controls based on the object and rights, or capabilities of a subject. For example, a table identifies the object, specifies access rights allowed for a subject, and permits access based on the user's posession of a capability (or ticket) for the object." CBK, pp. 191-192. To put it another way, as noted in AIO3 on p. 169, "A capabiltiy table is different from an ACL because the subject is bound to the capability table, whereas the object is bound to the ACL."
Again, a capability table could be used to implement the rules identified by an access control matrix but is different from the matrix itself.

CBK pp. 191-192, 317-318
AIO3, p. 169

QUESTION 127
Which access control model is best suited in an environment where a high security level is required and where it is desired that only the administrator grants access control?

A. DAC
B. MAC
C. Access control matrix
D. TACACS

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: MAC provides high security by regulating access based on the clearance of individual users and sensitivity labels for each object. Clearance levels and sensitivity levels cannot be modified by individual users -- for example, user Joe (SECRET clearance) cannot reclassify the "Presidential Doughnut Recipe" from "SECRET" to "CONFIDENTIAL" so that his friend Jane (CONFIDENTIAL clearance) can read it. The administrator is ultimately responsible for configuring this protection in accordance with security policy and directives from the Data Owner. DAC is incorrect. In DAC, the data owner is responsible for controlling access to the object. Access control matrix is incorrect. The access control matrix is a way of thinking about the access control needed by a population of subjects to a population of objects. This access control can be applied using rules, ACL's, capability tables, etc.
TACACS is incorrect. TACACS is a tool for performing user authentication.

CBK, p. 187, Domain 2: Access Control.
AIO3, Chapter 4, Access Control.

QUESTION 128
Which access control model provides upper and lower bounds of access capabilities for a subject?

A. Role-based access control
B. Lattice-based access control
C. Biba access control
D. Content-dependent access control

Correct Answer: B
Explanation

Explanation/Reference:

Explanation: In the lattice model, users are assigned security clearences and the data is classified. Access decisions are made based on the clearence of the user and the classification of the object. Lattice-based access control is an essential ingredient of formal security models such as Bell-LaPadula, Biba, Chinese Wall, etc.
The bounds concept comes from the formal definition of a lattice as a "partially ordered set for which every pair of elements has a greatest lower bound and a least upper bound." To see the application, consider a file classified as "SECRET" and a user Joe with a security clearence of "TOP SECRET." Under Bell-LaPadula, Joe's "least upper bound" access to the file is "READ" and his least lower bound is "NO WRITE" (star property).
Role-based access control is incorrect. Under RBAC, the access is controlled by the permissions assigned to a role and the specific role assigned to the user. Biba access control is incorrect. The Biba integrity model is based on a lattice structure but the context of the question disqualiifes it as the best answer. Content-dependent access control is incorrect. In content dependent access control, the actual content of the information determines access as enforced by the arbiter.

CBK, pp. 324-325.
AIO3, pp. 291-293. See aprticularly Figure 5-19 on p. 293 for an illustration of bounds in action.

QUESTION 129
How are memory cards and smart cards different?

A. Memory cards normally hold more memory than smart cards
B. Smart cards provide a two-factor authentication whereas memory cards don't
C. Memory cards have no processing power
D. Only smart cards can be used for ATM cards

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The main difference between memory cards and smart cards is their capacity to process information. A memory card holds information but cannot process information. A smart card holds information and has the necessary hardware and software to actually process that information.
A memory card holds a user's authentication information, so that this user needs only type in a user ID or PIN and presents the memory card to the system. If the entered information and the stored information match and are approved by an authentication service, the user is successfully authenticated.
A common example of a memory card is a swipe card used to provide entry to a building. The user enters a PIN and swipes the memory card through a card reader. If this is the correct combination, the reader flashes green and the individual can open the door and enter the building. Memory cards can also be used with computers, but they require a reader to process the information. The reader adds cost to the process, especially when one is needed for every computer. Additionally, the overhead of PIN and card generation adds additional overhead and complexity to the whole authentication process. However, a memory card provides a more secure authentication method than using only a password because the attacker would need to obtain the card and know the correct PIN.
Administrators and management need to weigh the costs and benefits of a memory card implementation as well as the security needs of the organization to determine if it is the right authentication mechanism for their environment.
One of the most prevalent weaknesses of memory cards is that data stored on the card are not protected. Unencrypted data on the card (or stored on the magnetic strip) can be extracted or copied. Unlike a smart card, where security controls and logic are embedded in the integrated circuit, memory cards do not employ an inherent mechanism to protect the data from exposure. Very little trust can be associated with confidentiality and integrity of information on the memory cards.
The following answers are incorrect:
"Smart cards provide two-factor authentication whereas memory cards don't" is incorrect. This is not necessarily true. A memory card can be combined with a pin or password to offer two factors authentication where something you have and something you know are used for factors. "Memory cards normally hold more memory than smart cards" is incorrect. While a memory card may or may not have more memory than a smart card, this is certainly not the best answer to the question.

"Only smart cards can be used for ATM cards" is incorrect. This depends on the decisions made by the particular institution and is not the best answer to the question.
Reference(s) used for this question:
Shon Harris, CISSP All In One, 6th edition , Access Control, Page 199 and also for people using the Kindle edition of the book you can look at Locations 4647-4650. Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Access Control ((ISC)2 Press) (Kindle Locations 2124-2139). Auerbach Publications. Kindle Edition.

QUESTION 130
Why do buffer overflows happen? What is the main cause?

A. Because buffers can only hold so much data
B. Because of improper parameter checking within the application
C. Because they are an easy weakness to exploit
D. Because of insufficient system memory

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Buffer Overflow attack takes advantage of improper parameter checking within the application. This is the classic form of buffer overflow and occurs because the programmer accepts whatever input the user supplies without checking to make sure that the length of the input is less than the size of the buffer in the program. The buffer overflow problem is one of the oldest and most common problems in software development and programming, dating back to the introduction of interactive computing. It can result when a program fills up the assigned buffer of memory with more data than its buffer can hold. When the program begins to write beyond the end of the buffer, the program's execution path can be changed, or data can be written into areas used by the operating system itself. This can lead to the insertion of malicious code that can be used to gain administrative privileges on the program or system.
As explained by Gaurab, it can become very complex. At the time of input even if you are checking the length of the input, it has to be check against the buffer size. Consider a case where entry point of data is stored in Buffer1 of Application1 and then you copy it to Buffer2 within Application2 later on, if you are just checking the length of data against Buffer1, it will not ensure that it will not cause a buffer overflow in Buffer2 of Application2.
A bit of reassurance from the ISC2 book about level of Coding Knowledge needed for the exam:
It should be noted that the CISSP is not required to be an expert programmer or know the inner workings of developing application software code, like the FORTRAN programming language, or how to develop Web applet code using Java. It is not even necessary that the CISSP know detailed security-specific coding practices such as the major divisions of buffer overflow exploits or the reason for preferring str(n)cpy to strcpy in the C language (although all such knowledge is, of course, helpful). Because the CISSP may be the person responsible for ensuring that security is included in such developments, the CISSP should know the basic procedures and concepts involved during the design and development of software programming. That is, in order for the CISSP to monitor the software development process and verify that security is included, the CISSP must understand the fundamental concepts of programming developments and the security strengths and weaknesses of various application development processes.
The following are incorrect answers:
"Because buffers can only hold so much data" is incorrect. This is certainly true but is not the best answer because the finite size of the buffer is not the problem -- the problem is that the programmer did not check the size of the input before moving it into the buffer. "Because they are an easy weakness to exploit" is incorrect. This answer is sometimes true but is not the best answer because the root cause of the buffer overflow is that the programmer did not check the size of the user input.
"Because of insufficient system memory" is incorrect. This is irrelevant to the occurrence of a buffer overflow.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 13319-13323). Auerbach Publications. Kindle Edition.

QUESTION 131
What is the main focus of the Bell-LaPadula security model?

A. Accountability
B. Integrity
C. Confidentiality
D. Availability

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The Bell-LaPadula model is a formal model dealing with confidentiality. The BellLaPadula Model (abbreviated BLP) is a state machine model used for enforcing access control in government and military applications. It was developed by David Elliott Bell and Leonard J. LaPadula, subsequent to strong guidance from Roger R. Schell to formalize the U.S. Department of Defense (DoD) multilevel security (MLS) policy. The model is a formal state transition model of computer security policy that describes a set of access control rules which use security labels on objects and clearances for subjects. Security labels range from the most sensitive (e.g."Top Secret"), down to the least sensitive (e.g., "Unclassified" or "Public"). The BellLaPadula model focuses on data confidentiality and controlled access to classified information, in contrast to the Biba Integrity Model which describes rules for the protection of data integrity. In this formal model, the entities in an information system are divided into subjects and objects.
The notion of a "secure state" is defined, and it is proven that each state transition preserves security by moving from secure state to secure state, thereby inductively proving that the system satisfies the security objectives of the model. The BellLaPadula model is built on the concept of a state machine with a set of allowable states in a computer network system. The transition from one state to another state is defined by transition functions. A system state is defined to be "secure" if the only permitted access modes of subjects to objects are in accordance with a security policy. To determine whether a specific access mode is allowed, the clearance of a subject is compared to the classification of the object (more precisely, to the combination of classification and set of compartments, making up the security level) to determine if the subject is authorized for the specific access mode. The clearance/classification scheme is expressed in terms of a lattice. The model defines two mandatory access control (MAC) rules and one discretionary access control (DAC) rule with three security properties:
The Simple Security Property - a subject at a given security level may not read an object at a higher security level (no read-up).
The -property (read "star"-property) - a subject at a given security level must not write to any object at a lower security level (no write-down). The -property is also known as the Confinement property.
The Discretionary Security Property - use of an access matrix to specify the discretionary access control.
The following are incorrect answers:
Accountability is incorrect. Accountability requires that actions be traceable to the user that performed them and is not addressed by the Bell-LaPadula model. Integrity is incorrect. Integrity is addressed in the Biba model rather than Bell-Lapadula. Availability is incorrect. Availability is concerned with assuring that data/ services are available to authorized users as specified in service level objectives and is not addressed by the Bell-Lapadula model.

CBK, pp. 325-326
AIO3, pp. 279 - 284
AIOv4 Security Architecture and Design (pages 333 - 336) AIOv5 Security Architecture and Design (pages 336 - 338) Wikipedia at https://en.wikipedia.org/wiki/Bell-La_Padula_model

QUESTION 132
Which of the following statements pertaining to the Bell-LaPadula is TRUE if you are NOT making use of the strong star property?

A. It allows "read up."
B. It addresses covert channels.
C. It addresses management of access controls.
D. It allows "write up."

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: BellLaPadula Confidentiality Model10 The BellLaPadula model is perhaps the most well-known and significant security model, in addition to being one of the oldest models used in the creation of modern secure computing systems. Like the Trusted Computer System Evaluation Criteria (or TCSEC), it was inspired by early U.S. Department of Defense security policies and the need to prove that confidentiality could be maintained. In other words, its primary goal is to prevent disclosure as the model system moves from one state (one point in time) to another.
When the strong star property is not being used it means that both the property and the Simple Security Property rules would be applied.
The Star (*) property rule of the Bell-LaPadula model says that subjects cannot write down, this would compromise the confidentiality of the information if someone at the secret layer would write the object down to a confidential container for example. The Simple Security Property rule states that the subject cannot read up which means that a subject at the secret layer would not be able to access objects at Top Secret for example.
You must remember: The model tells you about are NOT allowed to do. Anything else would be allowed. For example within the Bell LaPadula model you would be allowed to write up as it does not compromise the security of the information. In fact it would upgrade it to the point that you could lock yourself out of your own information if you have only a secret security clearance. The following are incorrect answers because they are all FALSE:
"It allows read up" is incorrect. The "simple security" property forbids read up. "It addresses covert channels" is incorrect. Covert channels are not addressed by the Bell- LaPadula model.
"It addresses management of access controls" is incorrect. Management of access controls are beyond the scope of the Bell-LaPadula model.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 17595-17600). Auerbach Publications. Kindle Edition.

QUESTION 133
Which security model introduces access to objects only through programs?

A. The Biba model
B. The Bell-LaPadula model
C. The Clark-Wilson model
D. The information flow model

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: In the Clark-Wilson model, the subject no longer has direct access to objects but instead must access them through programs (well -formed transactions). The ClarkWilson integrity model provides a foundation for specifying and analyzing an integrity policy for a computing system.
The model is primarily concerned with formalizing the notion of information integrity. Information integrity is maintained by preventing corruption of data items in a system due to either error or malicious intent. An integrity policy describes how the data items in the system should be kept valid from one state of the system to the next and specifies the capabilities of various principals in the system. The model defines enforcement rules and certification rules. ClarkWilson is more clearly applicable to business and industry processes in which the integrity of the information content is paramount at any level of classification.
Integrity goals of ClarkWilson model:
Prevent unauthorized users from making modification (Only this one is addressed by the Biba model).
Separation of duties prevents authorized users from making improper modifications. Well formed transactions: maintain internal and external consistency i.e. it is a series of operations that are carried out to transfer the data from one consistent state to the other.
The following are incorrect answers:
The Biba model is incorrect. The Biba model is concerned with integrity and controls access to objects based on a comparison of the security level of the subject to that of the object. The Bell-LaPdaula model is incorrect.

The Bell-LaPaula model is concerned with confidentiality and controls access to objects based on a comparison of the clearence level of the subject to the classification level of the object.
The information flow model is incorrect. The information flow model uses a lattice where objects are labelled with security classes and information can flow either upward or at the same level. It is similar in framework to the Bell-LaPadula model.

ISC2 Official Study Guide, Pages 325 - 327
AIO3, pp. 284 - 287
AIOv4 Security Architecture and Design (pages 338 - 342) AIOv5 Security Architecture and Design (pages 341 - 344) Wikipedia at: https://en.wikipedia.org/wiki/Clark-Wilson_model

QUESTION 134
Which security model ensures that actions that take place at a higher security level do not affect actions that take place at a lower level?

A. The Bell-LaPadula model
B. The information flow model
C. The noninterference model
D. The Clark-Wilson model

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The goal of a noninterference model is to strictly separate differing security levels to assure that higher-level actions do not determine what lower-level users can see. This is in contrast to other security models that control information flows between differing levels of users, By maintaining strict separation of security levels, a noninterference model minimizes leakages that might happen through a covert channel.
The model ensures that any actions that take place at a higher security level do not affect, or interfere with, actions that take place at a lower level. It is not concerned with the flow of data, but rather with what a subject knows about the state of the system. So if an entity at a higher security level performs an action, it can not change the state for the entity at the lower level.
The model also addresses the inference attack that occurs when some one has access to some type of information and can infer(guess) something that he does not have the clearance level or authority to know.
The following are incorrect answers:
The Bell-LaPadula model is incorrect. The Bell-LaPadula model is concerned only with confidentiality and bases access control decisions on the classfication of objects and the clearences of subjects.
The information flow model is incorrect. The information flow models have a similar framework to the Bell-LaPadula model and control how information may flow between objects based on security classes. Information will be allowed to flow only in accordance with the security policy. The Clark-Wilson model is incorrect. The Clark-Wilson model is concerned with change control and assuring that all modifications to objects preserve integrity by means of well-formed transactions and usage of an access triple (subjet - interface - object).

CBK, pp 325 - 326
AIO3, pp. 290 - 291
AIOv4 Security Architecture and Design (page 345)
AIOv5 Security Architecture and Design (pages 347 - 348) https://en.wikibooks.org/wiki/Security_Architecture_and_Design/Security_Models#Noninterference _Models

QUESTION 135
Which of the following security models does NOT concern itself with the flow of data?

A. The information flow model
B. The Biba model
C. The Bell-LaPadula model
D. The noninterference model

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The goal of a noninterference model is to strictly separate differing security levels to assure that higher-level actions do not determine what lower-level users can see. This is in contrast to other security models that control information flows between differing levels of users, By maintaining strict separation of security levels, a noninterference model minimizes leakages that might happen through a covert channel.
The Bell-LaPadula model is incorrect. The Bell-LaPadula model is concerned with confidentiality and bases access control decsions on the classfication of objects and the clearences of subjects. The information flow model is incorrect. The information flow models have a similar framework to the Bell-LaPadula model and control how information may flow between objects based on security classes.
The Biba model is incorrect. The Biba model is concerned with integrity and is a complement to the Bell-LaPadula model in that higher levels of integrity are more trusted than lower levels. Access control us based on these integrity levels to assure that read/write operations do not decrease an object's integrity.

CBK, pp 325 - 326
AIO3, pp. 290 - 291

QUESTION 136
What Orange Book security rating is reserved for systems that have been evaluated but fail to meet the criteria and requirements of the higher divisions?

A. A
B. D
C. E
D. F

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: D or "minimal protection" is reserved for systems that were evaluated under the TCSEC but did not meet the requirements for a higher trust level. A is incorrect. A or "Verified Protectection" is the highest trust level under the TCSEC. E is incorrect. The trust levels are A - D so "E" is not a valid trust level. F is incorrect. The trust levels are A - D so "F" is not a valid trust level.
CBK, pp. 329 - 330
AIO3, pp. 302 - 306

QUESTION 137
Which division of the Orange Book deals with discretionary protection (need-to-know)?

A. D
B. C
C. B
D. A

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: C deals with discretionary protection. See matric below:

TNI/TCSEC MATRIX

	A1	B3
DISCRETIONARY ACCESS		
Discretionary Access Control	▨	▨
Identification and Authentication	▨	▨
System Integrity	▨	▨
System Architecture	▨	▨
Security Testing	▨	▨
Security Features User's Guide Trusted Facility Manual Design Documentation Test Documentation	▨	▨
CONTROLLED ACCESS		
Protect Audit Trails	▨	▨
Object Reuse	▨	▨
MANDATORY ACCESS CONTROL		
Labels	▨	▨
Mandatory Access Control	▨	▨
Process isolation in system architecture	▨	▨
Design Specification & Verification	▨	▨
Device labels	▨	▨
Subject Sensitivity Labels	▨	▨
Trusted Path	▨	▨
Separation of Administrator and User functions	▨	▨
Covert Channel Analysis (Only Covert Storage Channel at B2)	▨	▨
Trusted Facility Management	▨	▨
Configuration Management	▨	▨
Trusted Recovery	▨	▨
Covert Channel Analysis (Both Timing and Covert Channel analysis at B3)	▨	▨
Security Administrator Role Defined	▨	▨
Monitor events and notify security personnel	▨	▨
Trusted Distribution	▨	
Formal Methods	▨	
	A1	B3

TCSEC Matric
The following are incorrect answers:
D is incorrect. D deals with minimal security.
B is incorrect. B deals with mandatory protection.
A is incorrect. A deals with verified protection.
Reference(s) used for this question:
CBK, p. 329 330
and
Shon Harris, CISSP All In One (AIO), 6th Edition , page 392-393

QUESTION 138
Which of the following are not Remote Access concerns?

A. Justification for remote access
B. Auditing of activities
C. Regular review of access privileges
D. Access badges

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Access badges are more relevant to physical security rather than remote access. "Justification for remote access" is incorrect. Justification for remote access is a relevant concern. "Auditing of activities" is incorrect. Auditing of activites is an imporant aspect to assure that malicious or unauthorized activities are not occuring. "Regular review of access privileges" is incorrect. Regular review of remote accept privileges is an important management responsibility.

AIO3, pp. 547 - 548

QUESTION 139
Smart cards are an example of which type of control?

A. Detective control
B. Administrative control
C. Technical control
D. Physical control

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Logical or technical controls involve the restriction of access to systems and the protection of information. Smart cards and encryption are examples of these types of control. Controls are put into place to reduce the risk an organization faces, and they come in three main flavors: administrative, technical, and physical. Administrative controls are commonly referred to as "soft controls" because they are more management-oriented. Examples of administrative controls are security documentation, risk management, personnel security, and training. Technical controls (also called logical controls) are software or hardware components, as in firewalls, IDS, encryption, identification and authentication mechanisms. And physical controls are items put into place to protect facility, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting.
Many types of technical controls enable a user to access a system and the resources within that system. A technical control may be a username and password combination, a Kerberos implementation, biometrics, public key infrastructure (PKI), RADIUS, TACACS +, or authentication using a smart card through a reader connected to a system. These technologies verify the user is who he says he is by using different types of authentication methods. Once a user is properly authenticated, he can be authorized and allowed access to

network resources.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 245). McGraw-Hill.
Kindle Edition.
and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 32).

QUESTION 140
What security model is dependent on security labels?

A. Discretionary access control
B. Label-based access control
C. Mandatory access control
D. Non-discretionary access control

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: With mandatory access control (MAC), the authorization of a subject's access to an object is dependant upon labels, which indicate the subject's clearance, and the classification or sensitivity of the object. Label-based access control is not defined. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 33).

QUESTION 141
What security model implies a central authority that define rules and sometimes global rules, dictating what subjects can have access to what objects?

A. Flow Model
B. Discretionary access control
C. Mandatory access control
D. Non-discretionary access control

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: As a security administrator you might configure user profiles so that users cannot change the system's time, alter system configuration files, access a command prompt, or install unapproved applications. This type of access control is referred to as nondiscretionary, meaning that access decisions are not made at the discretion of the user. Nondiscretionary access controls are put into place by an authoritative entity (usually a security administrator) with the goal of protecting the organization's most critical assets.
Non-discretionary access control is when a central authority determines what subjects can have access to what objects based on the organizational security policy. Centralized access control is not an existing security model.
Both, Rule Based Access Control (RuBAC or RBAC) and Role Based Access Controls (RBAC) falls into this category.
Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 221). McGraw-Hill.
Kindle Edition.
and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 33).

QUESTION 142

Which type of password token involves time synchronization?

A. Static password tokens
B. Synchronous dynamic password tokens
C. Asynchronous dynamic password tokens
D. Challenge-response tokens

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Synchronous dynamic password tokens generate a new unique password value at fixed time intervals, so the server and token need to be synchronized for the password to be accepted.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 37).
Also check out: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, chapter 4: Access Control (page 136).

QUESTION 143
Which of the following statements pertaining to biometrics is false?

A. Increased system sensitivity can cause a higher false rejection rate
B. The crossover error rate is the point at which false rejection rate equals the false acceptance rate.
C. False acceptance rate is also known as Type II error.
D. Biometrics are based on the Type 2 authentication mechanism.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Authentication is based on three factor types: type 1 is something you know, type 2 is something you have and type 3 is something you are. Biometrics are based on the Type 3 authentication mechanism.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 37).

QUESTION 144
Which of the following statements pertaining to Kerberos is TRUE?

A. Kerberos does not address availability
B. Kerberos does not address integrity
C. Kerberos does not make use of Symmetric Keys
D. Kerberos cannot address confidentiality of information

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The question was asking for a TRUE statement and the only correct statement is "Kerberos does not address availability".
Kerberos addresses the confidentiality and integrity of information. It does not directly address availability.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 42).

QUESTION 145
Which of the following centralized access control mechanisms is the least appropriate for mobile workers accessing the corporate network over analog lines?

A. TACACS
B. Call-back
C. CHAP
D. RADIUS

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Call-back allows for a distant user connecting into a system to be called back at a number already listed in a database of trusted users. The disadvantage of this system is that the user must be at a fixed location whose phone number is known to the authentication server. Being mobile workers, users are accessing the system from multiple locations, making call-back inappropriate for them.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 44).

QUESTION 146
Which of the following is NOT a compensating measure for access violations?

A. Backups
B. Business continuity planning
C. Insurance
D. Security awareness

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Security awareness is a preventive measure, not a compensating measure for access violations.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 50).

QUESTION 147
Which of the following is most affected by denial-of-service (DOS) attacks?

A. Confidentiality
B. Integrity
C. Accountability
D. Availability

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Denial of service attacks obviously affect availability of targeted systems. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 61).

QUESTION 148
What refers to legitimate users accessing networked services that would normally be restricted to them?

A. Spoofing
B. Piggybacking
C. Eavesdropping

D. Logon abuse

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Unauthorized access of restricted network services by the circumvention of security access controls is known as logon abuse. This type of abuse refers to users who may be internal to the network but access resources they would not normally be allowed. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 74).

QUESTION 149
In regards to information classification what is the main responsibility of information (data) owner?

A. determining the data sensitivity or classification level
B. running regular data backups
C. audit the data users
D. periodically check the validity and accuracy of the data

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Making the determination to decide what level of classification the information requires is the main responsibility of the data owner. The data owner within classification is a person from Management who has been entrusted with a data set that belong to the company. It could be for example the Chief Financial Officer (CFO) who has been entrusted with all financial date or it could be the Human Resource Director who has been entrusted with all Human Resource data. The information owner will decide what classification will be applied to the data based on Confidentiality, Integrity, Availability, Criticality, and Sensitivity of the data.
The Custodian is the technical person who will implement the proper classification on objects in accordance with the Data Owner. The custodian DOES NOT decide what classification to apply, it is the Data Owner who will dictate to the Custodian what is the classification to apply.
NOTE:
The term Data Owner is also used within Discretionary Access Control (DAC). Within DAC it means the person who has created an object. For example, if I create a file on my system then I am the owner of the file and I can decide who else could get access to the file. It is left to my discretion. Within DAC access is granted based solely on the Identity of the subject, this is why sometimes DAC is referred to as Identity Based Access Control.
The other choices were not the best answer
Running regular backups is the responsibility of custodian. Audit the data users is the responsibility of the auditors Periodically check the validity and accuracy of the data is not one of the data owner responsibility
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Page 14, Chapter 1: Security Management Practices.

QUESTION 150
Which of the following is not a two-factor authentication mechanism?

A. Something you have and something you know.
B. Something you do and a password.
C. A smartcard and something you are.
D. Something you know and a password.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Something you know and a password fits within only one of the three ways authentication could be done. A password is an example of something you know, thereby something you know and a password does not constitute a two-factor authentication as both are in the same category of factors.
A two-factor (strong) authentication relies on two different kinds of authentication factors out of a list of three possible choice:
something you know (e.g. a PIN or password),
something you have (e.g. a smart card, token, magnetic card), something you are is mostly Biometrics (e.g. a fingerprint) or something you do (e.g. signature dynamics).
TIP FROM CLEMENT:
On the real exam you can expect to see synonyms and sometimes sub-categories under the main categories. People are familiar with Pin, Passphrase, Password as subset of Something you know. However, when people see choices such as Something you do or Something you are they immediately get confused and they do not think of them as subset of Biometrics where you have Biometric implementation based on behavior and physilogical attributes. So something you do falls under the Something you are category as a subset.
Something your do would be signing your name or typing text on your keyboard for example. Strong authentication is simply when you make use of two factors that are within two different categories.
Reference(s) used for this question:
Shon Harris, CISSP All In One, Fifth Edition, pages 158-159

QUESTION 151
Which of the following access control models introduces user security clearance and data classification?

A. Role-based access control
B. Discretionary access control
C. Non-discretionary access control
D. Mandatory access control

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The mandatory access control model is based on a security label system. Users are given a security clearance and data is classified. The classification is stored in the security labels of the resources. Classification labels specify the level of trust a user must have to access a certain file.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 4: Access Control (Page 154).

QUESTION 152
Password management falls into which control category?

A. Compensating
B. Detective
C. Preventive
D. Technical

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Password management is an example of preventive control. Proper passwords prevent unauthorized users from accessing a system. There are literally hundreds of different access approaches, control methods, and technologies, both in the physical world and in the virtual electronic world. Each method addresses a different type of access control or a specific access need.
For example, access control solutions may incorporate identification and authentication mechanisms, filters, rules, rights, logging and monitoring, policy, and a plethora of other controls. However, despite the diversity of access control methods, all access control systems can be categorized into seven primary categories.

The seven main categories of access control are:
1. Directive: Controls designed to specify acceptable rules of behavior within an organization
2. Deterrent: Controls designed to discourage people from violating security directives
3. Preventive: Controls implemented to prevent a security incident or information breach
4. Compensating: Controls implemented to substitute for the loss of primary controls and mitigate risk down to an acceptable level
5. Detective: Controls designed to signal a warning when a security control has been breached
6. Corrective: Controls implemented to remedy circumstance, mitigate damage, or restore controls
7. Recovery: Controls implemented to restore conditions to normal after a security incident Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 1156-1176). Auerbach Publications. Kindle Edition.

QUESTION 153
Which of the following access control models requires security clearance for subjects?

A. Identity-based access control
B. Role-based access control
C. Discretionary access control
D. Mandatory access control

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: With mandatory access control (MAC), the authorization of a subject's access to an object is dependant upon labels, which indicate the subject's clearance. Identity-based access control is a type of discretionary access control. A role-based access control is a type of nondiscretionary access control.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 33).

QUESTION 154
Which of the following access control models requires defining classification for objects?

A. Role-based access control
B. Discretionary access control
C. Identity-based access control
D. Mandatory access control

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: With mandatory access control (MAC), the authorization of a subject's access to an object is dependant upon labels, which indicate the subject's clearance, and classification of objects.
The Following answers were incorrect:
Identity-based Access Control is a type of Discretionary Access Control (DAC), they are synonymous.
Role Based Access Control (RBAC) and Rule Based Access Control (RuBAC or RBAC) are types of Non Discretionary Access Control (NDAC).
Tip:
When you have two answers that are synonymous they are not the right choice for sure. There is only one access control model that makes use of Label, Clearances, and Categories, it is Mandatory Access Control, none of the other one makes use of those items.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 33).

QUESTION 155
In the context of access control, locks, gates, guards are examples of which of the following?

A. Administrative controls
B. Technical controls
C. Physical controls
D. Logical controls

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Administrative, technical and physical controls are categories of access control mechanisms.
Logical and Technical controls are synonymous. So both of them could be eliminated as possible choices.
Physical Controls: These are controls to protect the organization's people and physical environment, such as locks, gates, and guards. Physical controls may be called "operational controls" in some contexts.
Physical security covers a broad spectrum of controls to protect the physical assets (primarily the people) in an organization. Physical Controls are sometimes referred to as "operational" controls in some risk management frameworks. These controls range from doors, locks, and windows to environment controls, construction standards, and guards. Typically, physical security is based on the notion of establishing security zones or concentric areas within a facility that require increased security as you get closer to the valuable assets inside the facility. Security zones are the physical representation of the defense-in-depth principle discussed earlier in this chapter. Typically, security zones are associated with rooms, offices, floors, or smaller elements, such as a cabinet or storage locker. The design of the physical security controls within the facility must take into account the protection of the asset as well as the individuals working in that area.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 1301-1303). Auerbach Publications. Kindle Edition.
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 1312-1318). Auerbach Publications. Kindle Edition.

QUESTION 156
Which of the following statements pertaining to using Kerberos without any extension is false?

A. A client can be impersonated by password-guessing.
B. Kerberos is mostly a third-party authentication protocol.
C. Kerberos uses public key cryptography.
D. Kerberos provides robust authentication.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Kerberos is a trusted, credential-based, third-party authentication protocol that uses symmetric (secret) key cryptography to provide robust authentication to clients accessing services on a network.
Because a client's password is used in the initiation of the Kerberos request for the service protocol, password guessing can be used to impersonate a client. Here is a nice overview of HOW Kerberos is implement as described in RFC 4556:
1. Introduction
The Kerberos V5 protocol [RFC4120] involves use of a trusted third party known as the Key Distribution Center (KDC) to negotiate shared session keys between clients and services and provide mutual authentication between them.
The corner-stones of Kerberos V5 are the Ticket and the Authenticator. A Ticket encapsulates a symmetric key (the ticket session key) in an envelope (a public message) intended for a specific service. The contents of the Ticket are encrypted with a symmetric key shared between the service principal and the issuing KDC. The encrypted part of the Ticket contains the client principal name, among other items. An Authenticator is a record

that can be shown to have been recently generated using the ticket session key in the associated Ticket. The ticket session key is known by the client who requested the ticket. The contents of the Authenticator are encrypted with the associated ticket session key. The encrypted part of an Authenticator contains a timestamp and the client principal name, among other items.

As shown in Figure 1, below, the Kerberos V5 protocol consists of the following message exchanges between the client and the KDC, and the client and the application service:

The Authentication Service (AS) Exchange

The client obtains an "initial" ticket from the Kerberos authentication server (AS), typically a Ticket Granting Ticket (TGT). The AS-REQ message and the AS-REP message are the request and the reply message, respectively, between the client and the AS.

The Ticket Granting Service (TGS) Exchange

The client subsequently uses the TGT to authenticate and request a service ticket for a particular service, from the Kerberos ticket-granting server (TGS). The TGS-REQ message and the TGS-REP message are the request and the reply message respectively between the client and the TGS.

The Client/Server Authentication Protocol (AP) Exchange The client then makes a request with an AP-REQ message, consisting of a service ticket and an authenticator that certifies the client's possession of the ticket session key. The server may optionally reply with an AP-REP message. AP exchanges typically negotiate session-specific symmetric keys.

Usually, the AS and TGS are integrated in a single device also known as the KDC.

```
+--------------+
+--------->| KDC |
AS-REQ / +-------| |
/ / +--------------+
/ / ^ |
/ |AS-REP / |
| | / TGS-REQ + TGS-REP
| | / /
| | / /
| | / +---------+
| | / /
| | / /
| | / /
| v / v
++-------+------+ +-----------------+
| Client +------------>| Application |
| | AP-REQ | Server |
| |<------------| |
+---------------+ AP-REP +-----------------+
```

Figure 1: The Message Exchanges in the Kerberos V5 Protocol In the AS exchange, the KDC reply contains the ticket session key, among other items, that is encrypted using a key (the AS reply key) shared between the client and the KDC. The AS reply key is typically derived from the client's password for human users. Therefore, for human users, the attack resistance strength of the Kerberos protocol is no stronger than the strength of their passwords.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 40).

And

HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 4: Access Control (pages 147-151).

and

http://www.ietf.org/rfc/rfc4556.txt

QUESTION 157

Which of the following statements pertaining to Kerberos is false?

A. The Key Distribution Center represents a single point of failure.

B. Kerberos manages access permissions.

C. Kerberos uses a database to keep a copy of all users' public keys.

D. Kerberos uses symmetric key cryptography.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Kerberos is a trusted, credential-based, third-party authentication protocol that uses symmetric (secret) key cryptography to provide robust authentication to clients accessing services on a network.
One weakness of Kerberos is its Key Distribution Center (KDC), which represents a single point of failure.
The KDC contains a database that holds a copy of all of the symmetric/secret keys for the principals.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page40).

QUESTION 158
Which access control model would a lattice-based access control model be an example of?

A. Mandatory access control.
B. Discretionary access control.
C. Non-discretionary access control.
D. Rule-based access control.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: In a lattice model, there are pairs of elements that have the least upper bound of values and greatest lower bound of values. In a Mandatory Access Control (MAC) model, users and data owners do not have as much freedom to determine who can access files.
TIPS FROM CLEMENT
Mandatory Access Control is in place whenever you have permissions that are being imposed on the subject and the subject cannot arbitrarily change them. When the subject/owner of the file can change permissions at will, it is discretionary access control. Here is a breakdown largely based on explanations provided by Doug Landoll. I am reproducing below using my own word and not exactly how Doug explained it:
FIRST: The Lattice
A lattice is simply an access control tool usually used to implement Mandatory Access Control (MAC) and it could also be used to implement RBAC but this is not as common. The lattice model can be used for Integrity level or file permissions as well. The lattice has a least upper bound and greatest lower bound. It makes use of pair of elements such as the subject security clearance pairing with the object sensitivity label.
SECOND: DAC (Discretionary Access Control)
Let's get into Discretionary Access Control: It is an access control method where the owner (read the creator of the object) will decide who has access at his own discretion. As we all know, users are sometimes insane. They will share their files with other users based on their identity but nothing prevent the user from further sharing it with other users on the network. Very quickly you loose control on the flow of information and who has access to what. It is used in small and friendly environment where a low level of security is all that is required.
THIRD: MAC (Mandatory Access Control)
All of the following are forms of Mandatory Access Control:
Mandatory Access control (MAC) (Implemented using the lattice) You must remember that MAC makes use of Security Clearance for the subject and also Labels will be assigned to the objects. The clearance of the Subject must dominate (be equal or higher) the clearance of the Object being accessed. The label attached to the object will indicate the sensitivity leval and the categories the object belongs to. The categories are used to implement the Need to Know.
All of the following are forms of Non Discretionary Access Control:
Role Based Access Control (RBAC)
Rule Based Access Control (Think Firewall in this case) The official ISC2 book says that RBAC (synonymous with Non Discretionary Access Control) is a form of DAC but they are simply wrong. RBAC is a form of Non Discretionary Access Control. Non Discretionary DOES NOT equal mandatory access control as there is no labels and clearance involved.

I hope this clarifies the whole drama related to what is what in the world of access control. In the same line of taught, you should be familiar with the difference between Explicit permission (the user has his own profile) versus Implicit (the user inherit permissions by being a member of a role for example).
The following answers are incorrect:
Discretionary access control. Is incorrect because in a Discretionary Access Control (DAC) model, access is restricted based on the authorization granted to the users. It is identity based access control only. It does not make use of a lattice.
Non-discretionary access control. Is incorrect because Non-discretionary Access Control (NDAC) uses the role-based access control method to determine access rights and permissions. It is often times used as a synonym to RBAC which is Role Based Access Control. The user inherit permission from the role when they are assigned into the role. This type of access could make use of a lattice but could also be implemented without the use of a lattice in some case. Mandatory Access Control was a better choice than this one, but RBAC could also make use of a lattice. The BEST answer was MAC.
Rule-based access control. Is incorrect because it is an example of a Non-discretionary Access Control (NDAC) access control mode. You have rules that are globally applied to all users. There is no such thing as a lattice being use in Rule-Based Access Control.

AIOv3 Access Control (pages 161 - 168)
AIOv3 Security Models and Architecture (pages 291 - 293)

QUESTION 159
Which of the following is an example of discretionary access control?

A. Identity-based access control
B. Task-based access control
C. Role-based access control
D. Rule-based access control

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: An identity-based access control is an example of discretionary access control that is based on an individual's identity. Identity-based access control (IBAC) is access control based on the identity of the user (typically relayed as a characteristic of the process acting on behalf of that user) where access authorizations to specific objects are assigned based on user identity. Rule Based Access Control (RuBAC) and Role Based Access Control (RBAC) are examples of non-discretionary access controls.
Rule-based access control is a type of non-discretionary access control because this access is determined by rules and the subject does not decide what those rules will be, the rules are uniformly applied to ALL of the users or subjects.
In general, all access control policies other than DAC are grouped in the category of nondiscretionary access control (NDAC). As the name implies, policies in this category have rules that are not established at the discretion of the user. Non-discretionary policies establish controls that cannot be changed by users, but only through administrative action. Both Role Based Access Control (RBAC) and Rule Based Access Control (RuBAC) fall within Non Discretionary Access Control (NDAC). If it is not DAC or MAC then it is most likely NDAC. BELOW YOU HAVE A DESCRIPTION OF THE DIFFERENT CATEGORIES:
MAC = Mandatory Access Control
Under a mandatory access control environment, the system or security administrator will define what permissions subjects have on objects. The administrator does not dictate user's access but simply configure the proper level of access as dictated by the Data Owner. The MAC system will look at the Security Clearance of the subject and compare it with the object sensitivity level or classification level. This is what is called the dominance relationship. The subject must DOMINATE the object sensitivity level. Which means that the subject must have a security clearance equal or higher than the object he is attempting to access. MAC also introduce the concept of labels. Every objects will have a label attached to them indicating the classification of the object as well as categories that are used to impose the need to know (NTK) principle. Even thou a user has a security clearance of Secret it does not mean he would be able to access any Secret documents within the system. He would be allowed to access only Secret document for which he has a Need To Know, formal approval, and object where the user belong to one of the categories attached to the object. If there is no

clearance and no labels then IT IS NOT Mandatory Access Control. Many of the other models can mimic MAC but none of them have labels and a dominance relationship so they are NOT in the MAC category.
DAC = Discretionary Access Control
DAC is also known as: Identity Based access control system. The owner of an object is define as the person who created the object. As such the owner has the discretion to grant access to other users on the network. Access will be granted based solely on the identity of those users.
Such system is good for low level of security. One of the major problem is the fact that a user who has access to someone's else file can further share the file with other users without the knowledge or permission of the owner of the file. Very quickly this could become the wild wild west as there is no control on the dissimination of the information.
RBAC = Role Based Access Control
RBAC is a form of Non-Discretionary access control.
Role Based access control usually maps directly with the different types of jobs performed by employees within a company.
For example there might be 5 security administrator within your company. Instead of creating each of their profile one by one, you would simply create a role and assign the administrators to the role. Once an administrator has been assigned to a role, he will IMPLICITLY inherit the permissions of that role.
RBAC is great tool for environment where there is a a large rotation of employees on a daily basis such as a very large help desk for example.
RBAC or RuBAC = Rule Based Access Control
RuBAC is a form of Non-Discretionary access control.
A good example of a Rule Based access control device would be a Firewall. A single set of rules is imposed to all users attempting to connect through the firewall. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.
and
NISTIR-7316 at http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf and
http://itlaw.wikia.com/wiki/Identity-based_access_control

QUESTION 160
Which of the following would be used to implement Mandatory Access Control (MAC)?

A. Clark-Wilson Access Control
B. Role-based access control
C. Lattice-based access control
D. User dictated access control

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The lattice is a mechanism use to implement Mandatory Access Control (MAC) Under Mandatory Access Control (MAC) you have:
Mandatory Access Control
Under Non Discretionary Access Control (NDAC) you have:
Rule-Based Access Control
Role-Based Access Control
Under Discretionary Access Control (DAC) you have:
Discretionary Access Control
The Lattice Based Access Control is a type of access control used to implement other access control method. A lattice is an ordered list of elements that has a least upper bound and a most lower bound. The lattice can be used for MAC, DAC, Integrity level, File Permission, and more For example in the case of MAC, if we look at common government classifications, we have the following:
TOP SECRET
SECRET -----------------------I am the user at secret
CONFIDENTIAL
SENSITIVE BUT UNCLASSIFIED
UNCLASSIFIED
If you look at the diagram above where I am a user at SECRET it means that I can access document at lower

classification but not document at TOP SECRET. The lattice is a list of ORDERED ELEMENT, in this case the ordered elements are classification levels. My least upper bound is SECRET and my most lower bound is UNCLASSIFIED. However the lattice could also be used for Integrity Levels such as:
VERY HIGH
HIGH
MEDIUM ----------I am a user, process, application at the medium level LOW
VERY LOW
In the case of of Integrity levels you have to think about TRUST. Of course if I take for example the the VISTA operating system which is based on Biba then Integrity Levels would be used. As a user having access to the system I cannot tell a process running with administrative privilege what to do. Else any users on the system could take control of the system by getting highly privilege process to do things on their behalf. So no read down would be allowed in this case and this is an example of the Biba model.
Last but not least the lattice could be use for file permissions:
RWX
RW ---------User at this level
R
If I am a user with READ and WRITE (RW) access privilege then I cannot execute the file because I do not have execute permission which is the X under linux and UNIX. Many people confuse the Lattice Model and many books says MAC = LATTICE, however the lattice can be use for other purposes.
There is also Role Based Access Control (RBAC) that exists out there. It COULD be used to simulate MAC but it is not MAC as it does not make use of Label on objects indicating sensitivity and categories. MAC also require a clearance that dominates the object. You can get more info about RBAC at:http://csrc.nist.gov/groups/SNS/rbac/faq.html#03 Also note that many book uses the same acronym for Role Based Access Control and Rule Based Access Control which is RBAC, this can be confusing.
The proper way of writing the acronym for Rule Based Access Control is RuBAC, unfortunately it is not commonly used.

There is a great article on technet that talks about the lattice in VISTA:
http://blogs.technet.com/b/steriley/archive/2006/07/21/442870.aspx also see:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 33).
and
http://www.microsoft-watch.com/content/vista/gaging_vistas_integrity.html

QUESTION 161
Which type of attack involves impersonating a user or a system?

A. Smurfing attack
B. Spoofing attack
C. Spamming attack
D. Sniffing attack

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: A spoofing attack is when an attempt is made to gain access to a computer system by posing as an authorized user or system. Spamming refers to sending out or posting junk advertising and unsolicited mail. A smurf attack is a type of denial-of-service attack using PING and a spoofed address. Sniffing refers to observing packets passing on a network. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 77).

QUESTION 162
Which of the following is NOT an advantage that TACACS+ has over TACACS?

A. Event logging
B. Use of two-factor password authentication

C. User has the ability to change his password

D. Ability for security tokens to be resynchronized

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Although TACACS+ provides better audit trails, event logging is a service that is provided with TACACS.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 121).

QUESTION 163
Which of the following remote access authentication systems is the most robust?

A. TACACS+

B. RADIUS

C. PAP

D. TACACS

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: TACACS+ is a proprietary Cisco enhancement to TACACS and is more robust than RADIUS. PAP is not a remote access authentication system but a remote node security protocol. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 122).

QUESTION 164
Which of the following is an example of a passive attack?

A. Denying services to legitimate users

B. Shoulder surfing

C. Brute-force password cracking

D. Smurfing

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Shoulder surfing is a form of a passive attack involving stealing passwords, personal identification numbers or other confidential information by looking over someone's shoulder. All other forms of attack are active attacks, where a threat makes a modification to the system in an attempt to take advantage of a vulnerability.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 3: Security Management Practices (page 63).

QUESTION 165
What does the Clark-Wilson security model focus on?

A. Confidentiality

B. Integrity

C. Accountability

D. Availability

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The Clark-Wilson model addresses integrity. It incorporates mechanisms to enforce internal and external consistency, a separation of duty, and a mandatory integrity policy. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architectures and Models (page 205).

QUESTION 166
What does the simple security (ss) property mean in the Bell-LaPadula model?

A. No read up
B. No write down
C. No read down
D. No write up

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The ss (simple security) property of the Bell-LaPadula access control model states that reading of information by a subject at a lower sensitivity level from an object at a higher sensitivity level is not permitted (no read up).
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architectures and Models (page 202).

QUESTION 167
What does the (star) property mean in the Bell-LaPadula model?

A. No write up
B. No read up
C. No write down
D. No read down

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The (star) property of the Bell-LaPadula access control model states that writing of information by a subject at a higher level of sensitivity to an object at a lower level of sensitivity is not permitted (no write down).
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architectures and Models (page 202).
Also check out: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, Chapter 5: Security Models and Architecture (page 242, 243).

QUESTION 168
What does the (star) integrity axiom mean in the Biba model?

A. No read up
B. No write down
C. No read down

D. No write up

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The (star) integrity axiom of the Biba access control model states that an object at one level of integrity is not permitted to modify an object of a higher level of integrity (no write up). Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architectures and Models (page 205).

QUESTION 169
What does the simple integrity axiom mean in the Biba model?

A. No write down
B. No read down
C. No read up
D. No write up

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The simple integrity axiom of the Biba access control model states that a subject at one level of integrity is not permitted to observe an object of a lower integrity (no read down). Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architectures and Models (page 205).

QUESTION 170
What is the Biba security model concerned with?

A. Confidentiality
B. Reliability
C. Availability
D. Integrity

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The Biba security model addresses the integrity of data being threatened when subjects at lower security levels are able to write to objects at higher security levels and when subjects can read data at lower levels.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 5: Security Models and Architecture (Page 244).

QUESTION 171
Which security model uses division of operations into different parts and requires different users to perform each part?

A. Bell-LaPadula model
B. Biba model
C. Clark-Wilson model
D. Non-interference model

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The Clark-Wilson model uses separation of duties, which divides an operation into different parts and requires different users to perform each part. This prevents authorized users from making unauthorized modifications to data, thereby protecting its integrity. The Clark-Wilson integrity model provides a foundation for specifying and analyzing an integrity policy for a computing system.
The model is primarily concerned with formalizing the notion of information integrity. Information integrity is maintained by preventing corruption of data items in a system due to either error or malicious intent. An integrity policy describes how the data items in the system should be kept valid from one state of the system to the next and specifies the capabilities of various principals in the system. The model defines enforcement rules and certification rules. The model's enforcement and certification rules define data items and processes that provide the basis for an integrity policy. The core of the model is based on the notion of a transaction. A well-formed transaction is a series of operations that transition a system from one consistent state to another consistent state.
In this model the integrity policy addresses the integrity of the transactions. The principle of separation of duty requires that the certifier of a transaction and the implementer be different entities.
The model contains a number of basic constructs that represent both data items and processes that operate on those data items. The key data type in the Clark-Wilson model is a Constrained Data Item (CDI). An Integrity Verification Procedure (IVP) ensures that all CDIs in the system are valid at a certain state.
Transactions that enforce the integrity policy are represented by Transformation Procedures (TPs). A TP takes as input a CDI or Unconstrained Data Item (UDI) and produces a CDI. A TP must transition the system from one valid state to another valid state. UDIs represent system input (such as that provided by a user or adversary). A TP must guarantee (via certification) that it transforms all possible values of a UDI to a "safe" CDI. In general, preservation of data integrity has three goals:
Prevent data modification by unauthorized parties
Prevent unauthorized data modification by authorized parties Maintain internal and external consistency (i.e. data reflects the real world) Clark-Wilson addresses all three rules but BIBA addresses only the first rule of intergrity.

HARRIS, Shon, All-In-One CISSP Certification Fifth Edition, McGraw-Hill/Osborne, Chapter 5:
Security Architecture and Design (Page 341-344).
and
http://en.wikipedia.org/wiki/Clark-Wilson_model

QUESTION 172
What is the main objective of proper separation of duties?

A. To prevent employees from disclosing sensitive information.
B. To ensure access controls are in place.
C. To ensure that no single individual can compromise a system.
D. To ensure that audit trails are not tampered with.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The primary objective of proper separation of duties is to ensure that one person acting alone cannot compromise the company's security in any way. A proper separation of duties does not prevent employees from disclosing information, nor does it ensure that access controls are in place or that audit trails are not tampered with. Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/ Osborne, 2002, Chapter 12: Operations Security (Page 808).

QUESTION 173
Which of the following is related to physical security and is not considered a technical control?

A. Access control Mechanisms

B. Intrusion Detection Systems

C. Firewalls

D. Locks

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: All of the above are considered technical controls except for locks, which are physical controls.
Administrative, Technical, and Physical Security Controls Administrative security controls are primarily policies and procedures put into place to define and guide employee actions in dealing with the organization's sensitive information. For example, policy might dictate (and procedures indicate how) that human resources conduct background checks on employees with access to sensitive information. Requiring that information be classified and the process to classify and review information classifications is another example of an administrative control. The organization security awareness program is an administrative control used to make employees cognizant of their security roles and responsibilities. Note that administrative security controls in the form of a policy can be enforced or verified with technical or physical security controls. For instance, security policy may state that computers without antivirus software cannot connect to the network, but a technical control, such as network access control software, will check for antivirus software when a computer tries to attach to the network. Technical security controls (also called logical controls) are devices, processes, protocols, and other measures used to protect the C.I.
A. of sensitive information. Examples include logical
access systems, encryptions systems, antivirus systems, firewalls, and intrusion detection systems.
Physical security controls are devices and means to control physical access to sensitive information and to protect the availability of the information. Examples are physical access systems (fences, mantraps, guards), physical intrusion detection systems (motion detector, alarm system), and physical protection systems (sprinklers, backup generator). Administrative and technical controls depend on proper physical security controls being in place. An administrative policy allowing only authorized employees access to the data center do little good without some kind of physical access control.
From the GIAC.ORG website

QUESTION 174
Which of the following floors would be most appropriate to locate information processing facilities in a 6-stories building?

A. Basement

B. Ground floor

C. Third floor

D. Sixth floor

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: You data center should be located in the middle of the facility or the core of a building to provide protection from natural disasters or bombs and provide easier access to emergency crewmembers if necessary. By being at the core of the facility the external wall would act as a secondary layer of protection as well.
Information processing facilities should not be located on the top floors of buildings in case of a fire or flooding coming from the roof. Many crimes and theft have also been conducted by simply cutting a large hole on the roof.
They should not be in the basement because of flooding where water has a natural tendancy to flow down :-) Even a little amount of water would affect your operation considering the quantity of electrical cabling sitting directly on the cement floor under under your raise floor. The data center should not be located on the first floor due to the presence of the main entrance where people are coming in and out. You have a lot of high traffic areas such as the elevators, the loading docks, cafeteria, coffee shopt, etc.. Really a bad location for a data center. So it was easy to come up with the answer by using the process of elimination where the top, the

bottom, and the basement are all bad choices. That left you with only one possible answer which is the third floor.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 5th Edition, Page 425.

QUESTION 175
Which of the following Operation Security controls is intended to prevent unauthorized intruders from internally or externally accessing the system, and to lower the amount and impact of unintentional errors that are entering the system?

A. Detective Controls
B. Preventative Controls
C. Corrective Controls
D. Directive Controls

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: In the Operations Security domain, Preventative Controls are designed to prevent unauthorized intruders from internally or externally accessing the system, and to lower the amount and impact of unintentional errors that are entering the system. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 217.

QUESTION 176
This baseline sets certain thresholds for specific errors or mistakes allowed and the amount of these occurrences that can take place before it is considered suspicious?

A. Checkpoint level
B. Ceiling level
C. Clipping level
D. Threshold level

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Organizations usually forgive a particular type, number, or pattern of violations, thus permitting a predetermined number of user errors before gathering this data for analysis. An organization attempting to track all violations, without sophisticated statistical computing ability, would be unable to manage the sheer quantity of such data. To make a violation listing effective, a clipping level must be established.
The clipping level establishes a baseline for violation activities that may be normal user errors. Only after this baseline is exceeded is a violation record produced. This solution is particularly effective for small- to medium-sized installations. Organizations with large-scale computing facilities often track all violations and use statistical routines to cull out the minor infractions (e.g., forgetting a password or mistyping it several times).
If the number of violations being tracked becomes unmanageable, the first step in correcting the problems should be to analyze why the condition has occurred. Do users understand how they are to interact with the computer resource? Are the rules too difficult to follow? Violation tracking and analysis can be valuable tools in assisting an organization to develop thorough but useable controls. Once these are in place and records are produced that accurately reflect serious violations, tracking and analysis become the first line of defense. With this procedure, intrusions are discovered before major damage occurs and sometimes early enough to catch the perpetrator. In addition, business protection and preservation are strengthened.
The following answers are incorrect:
All of the other choices presented were simply detractors. The following reference(s) were used for this question:
Handbook of Information Security Management

QUESTION 177

Which type of control is concerned with avoiding occurrences of risks?

A. Deterrent controls
B. Detective controls
C. Preventive controls
D. Compensating controls

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Preventive controls are concerned with avoiding occurrences of risks while deterrent controls are concerned with discouraging violations. Detecting controls identify occurrences and compensating controls are alternative controls, used to compensate weaknesses in other controls.
Supervision is an example of compensating control.
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 178
Which type of control is concerned with restoring controls?

A. Compensating controls
B. Corrective controls
C. Detective controls
D. Preventive controls

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Corrective controls are concerned with remedying circumstances and restoring controls.
Detective controls are concerned with investigating what happen after the fact such as logs and video surveillance tapes for example.
Compensating controls are alternative controls, used to compensate weaknesses in other controls.
Preventive controls are concerned with avoiding occurrences of risks. Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 179
Which of the following biometric parameters are better suited for authentication use over a long period of time?

A. Iris pattern
B. Voice pattern
C. Signature dynamics
D. Retina pattern

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The iris pattern is considered lifelong. Unique features of the iris are: freckles, rings, rifts, pits, striations, fibers, filaments, furrows, vasculature and coronas. Voice, signature and retina patterns are more likely to change over time, thus are not as suitable for authentication over a long period of time without needing re-enrollment.
Source: FERREL, Robert G, questions and Answers for the CISSP Exam, domain 1 (derived from the Information Security Management Handbook, 4th Ed., by Tipton & Krause).

QUESTION 180

In the CIA triad, what does the letter A stand for?

A. Auditability
B. Accountability
C. Availability
D. Authentication

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The CIA triad stands for Confidentiality, Integrity and Availability.

QUESTION 181
Which TCSEC class specifies discretionary protection?

A. B2
B. B1
C. C2
D. C1

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: C1 involves discretionary protection, C2 involves controlled access protection, B1 involves labeled security protection and B2 involves structured protection. Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 182
Which of the following access control techniques best gives the security officers the ability to specify and enforce enterprise-specific security policies in a way that maps naturally to an organization's structure?

A. Access control lists
B. Discretionary access control
C. Role-based access control
D. Non-mandatory access control

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Role-based access control (RBAC) gives the security officers the ability to specify and enforce enterprise-specific security policies in a way that maps naturally to an organization's structure. Each user is assigned one or more roles, and each role is assigned one or more privileges that are given to users in that role. An access control list (ACL) is a table that tells a system which access rights each user has to a particular system object. With discretionary access control, administration is decentralized and owners of resources control other users' access. Nonmandatory access control is not a defined access control technique. Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 2: Access Control Systems and Methodology (page 9).

QUESTION 183
Which access control model was proposed for enforcing access control in government and military applications?

A. Bell-LaPadula model
B. Biba model
C. Sutherland model
D. Brewer-Nash model

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The Bell-LaPadula model, mostly concerned with confidentiality, was proposed for enforcing access control in government and military applications. It supports mandatory access control by determining the access rights from the security levels associated with subjects and objects. It also supports discretionary access control by checking access rights from an access matrix. The Biba model, introduced in 1977, the Sutherland model, published in 1986, and the Brewer-Nash model, published in 1989, are concerned with integrity. Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 2: Access Control Systems and Methodology (page 11).

QUESTION 184
Which access control model achieves data integrity through well-formed transactions and separation of duties?

A. Clark-Wilson model
B. Biba model
C. Non-interference model
D. Sutherland model

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The Clark-Wilson model differs from other models that are subject- and objectoriented by introducing a third access element programs resulting in what is called an access triple, which prevents unauthorized users from modifying data or programs. The Biba model uses objects and subjects and addresses integrity based on a hierarchical lattice of integrity levels. The non-interference model is related to the information flow model with restrictions on the information flow. The Sutherland model approaches integrity by focusing on the problem of inference. Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 2: Access Control Systems and Methodology (page 12).
And: KRAUSE, Micki & TIPTON, Harold F., Handbook of Information Security Management, CRC Press, 1997, Domain 1: Access Control.

QUESTION 185
For maximum security design, what type of fence is most effective and cost-effective method (Foot are being used as measurement unit below)?

A. 3' to 4' high
B. 6' to 7' high
C. 8' high and above with strands of barbed wire
D. Double fencing

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The most commonly used fence is the chain linked fence and it is the most affordable. The standard is a six-foot high fence with two-inch mesh square openings. The material should consist of nine-gauge vinyl or galvanized metal. Nine-gauge is a typical fence material installed in residential areas. Additionally, it is recommended to place barbed wire strands angled out from the top of the fence at a 45°

angle and away from the protected area with three strands running across the top. This will provide for a seven-foot fence. There are several variations of the use of "top guards" using Vshaped barbed wire or the use of concertina wire as an enhancement, which has been a replacement for more traditional three strand barbed wire "top guards." The fence should be fastened to ridged metal posts set in concrete every six feet with additional bracing at the corners and gate openings. The bottom of the fence should be stabilized against intruders crawling under by attaching posts along the bottom to keep the fence from being pushed or pulled up from the bottom. If the soil is sandy, the bottom edge of the fence should be installed below ground level.
For maximum security design, the use of double fencing with rolls of concertina wire positioned between the two fences is the most effective deterrent and cost-efficient method. In this design, an intruder is required to use an extensive array of ladders and equipment to breach the fences. Most fencing is largely a psychological deterrent and a boundary marker rather than a barrier, because in most cases such fences can be rather easily penetrated unless added security measures are taken to enhance the security of the fence. Sensors attached to the fence to provide electronic monitoring of cutting or scaling the fence can be used.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 24416-24431). Auerbach Publications. Kindle Edition.

QUESTION 186
Which of the following protection devices is used for spot protection within a few inches of the object, rather than for overall room security monitoring?

A. Wave pattern motion detectors
B. Capacitance detectors
C. Field-powered devices
D. Audio detectors

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Capacitance detectors monitor an electrical field surrounding the object being monitored. They are used for spot protection within a few inches of the object, rather than for overall room security monitoring used by wave detectors. Penetration of this field changes the electrical capacitance of the field enough to generate and alarm. Wave pattern motion detectors generate a frequency wave pattern and send an alarm if the pattern is disturbed as it is reflected back to its receiver. Field-powered devices are a type of personnel access control devices. Audio detectors simply monitor a room for any abnormal sound wave generation and trigger an alarm. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 10: Physical security (page 344).

QUESTION 187
Physical security is accomplished through proper facility construction, fire and water protection, anti-theft mechanisms, intrusion detection systems, and security procedures that are adhered to and enforced. Which of the following is not a component that achieves this type of security?

A. Administrative control mechanisms
B. Integrity control mechanisms
C. Technical control mechanisms
D. Physical control mechanisms

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Integrity Controls Mechanisms are not part of physical security. All of the other detractors were correct this one was the wrong one that does not belong to Physical Security. Below you have more details extracted from the SearchSecurity web site:
Information security depends on the security and management of the physical space in which computer

systems operate. Domain 9 of the CISSP exam's Common Body of Knowledge addresses the challenges of securing the physical space, its systems and the people who work within it by use of administrative, technical and physical controls. The following question NO: s are covered:

Facilities management: The administrative processes that govern the maintenance and protection of the physical operations space, from site selection through emergency response. Risks, issues and protection strategies: Risk identification and the selection of security protection components.

Perimeter security: Typical physical protection controls.

Facilities management

Facilities management is a complex component of corporate security that ranges from the planning of a secure physical site to the management of the physical information system environment. Facilities management responsibilities include site selection and physical security planning (i.e. facility construction, design and layout, fire and water damage protection, antitheft mechanisms, intrusion detection and security procedures.)

Protections must extend to both people and assets. The necessary level of protection depends on the value of the assets and data. CISSP® candidates must learn the concept of critical-path analysis as a means of determining a component's business function criticality relative to the cost of operation and replacement. Furthermore, students need to gain an understanding of the optimal location and physical attributes of a secure facility. Among the question NO: s covered in this domain are site inspection, location, accessibility and obscurity, considering the area crime rate, and the likelihood of natural hazards such as floods or earthquakes.

This domain also covers the quality of construction material, such as its protective qualities and load capabilities, as well as how to lay out the structure to minimize risk of forcible entry and accidental damage.

Regulatory compliance is also touched on, as is preferred proximity to civil protection services, such as fire and police stations. Attention is given to computer and equipment rooms, including their location, configuration (entrance/egress requirements) and their proximity to wiring distribution centers at the site.

Physical risks, issues and protection strategies

An overview of physical security risks includes risk of theft, service interruption, physical damage, compromised system integrity and unauthorized disclosure of information. Interruptions to business can manifest due to loss of power, services, telecommunications connectivity and water supply. These can also seriously compromise electronic security monitoring alarm/response devices. Backup options are also covered in this domain, as is a strategy for quantifying the risk exposure by simple formula.

Investment in preventive security can be costly. Appropriate redundancy of people skills, systems and infrastructure must be based on the criticality of the data and assets to be preserved. Therefore a strategy is presented that helps determine the selection of cost appropriate controls. Among the question NO: s covered in this domain are regulatory and legal requirements, common standard security protections such as locks and fences, and the importance of establishing service level agreements for maintenance and disaster support. Rounding out the optimization approach are simple calculations for determining mean time between failure and mean time to repair (used to estimate average equipment life expectancy) -- essential for estimating the cost/ benefit of purchasing and maintaining redundant equipment. As the lifeblood of computer systems, special attention is placed on adequacy, quality and protection of power supplies. CISSP candidates need to understand power supply concepts and terminology, including those for quality (i.e. transient noise vs. clean power); types of interference (EMI and RFI); and types of interruptions such as power excess by spikes and surges, power loss by fault or blackout, and power degradation from sags and brownouts. A simple formula is presented for determining the total cost per hour for backup power. Proving power reliability through testing is recommended and the advantages of three power protection approaches are discussed (standby UPS, power line conditioners and backup sources) including minimum requirements for primary and alternate power provided. Environmental controls are explored in this domain, including the value of positive pressure water drains and climate monitoring devices used to control temperature, humidity and reduce static electricity. Optimal temperatures and humidity settings are provided. Recommendations include strict procedures during emergencies, preventing typical risks (such as blocked fans), and the use of antistatic armbands and hygrometers. Positive pressurization for proper ventilation and monitoring for air born contaminants is stressed.

The pros and cons of several detection response systems are deeply explored in this domain. The concept of combustion, the classes of fire and fire extinguisher ratings are detailed. Mechanisms behind smoke-activated, heat-activated and flame-activated devices and Automatic Dial-up alarms are covered, along with their advantages, costs and shortcomings. Types of fire sources are distinguished and the effectiveness of fire suppression methods for each is included. For instance, Halon and its approved replacements are covered, as are the advantages and the inherent risks to equipment of the use of water sprinklers.

Administrative controls

The physical security domain also deals with administrative controls applied to physical sites and assets. The need for skilled personnel, knowledge sharing between them, separation of duties, and appropriate oversight

in the care and maintenance of equipment and environments is stressed. A list of management duties including hiring checks, employee maintenance activities and recommended termination procedures is offered. Emergency measures include accountability for evacuation and system shutdown procedures, integration with disaster and business continuity plans, assuring documented procedures are easily available during different types of emergencies, the scheduling of periodic equipment testing, administrative reviews of documentation, procedures and recovery plans, responsibilities delegation, and personnel training and drills.
Perimeter security
Domain nine also covers the devices and techniques used to control access to a space. These include access control devices, surveillance monitoring, intrusion detection and corrective actions. Specifications are provided for optimal external boundary protection, including fence heights and placement, and lighting placement and types. Selection of door types and lock characteristics are covered. Surveillance methods and intrusion-detection methods are explained, including the use of video monitoring, guards, dogs, proximity detection systems, photoelectric/photometric systems, wave pattern devices, passive infrared systems, and sound and motion detectors, and current flow sensitivity devices that specifically address computer theft. Room lock types -- both preset and cipher locks (and their variations) -- device locks, such as portable laptop locks, lockable server bays, switch control locks and slot locks, port controls, peripheral switch controls and cable trap locks are also covered. Personal access control methods used to identify authorized users for site entry are covered at length, noting social engineering risks such as piggybacking. Wireless proximity devices, both user access and system sensing readers are covered (i.e. transponder based, passive devices and field powered devices) in this domain. Now that you've been introduced to the key concepts of Domain 9, watch the Domain 9, Physical Security video
Return to the CISSP Essentials Security School main page See all SearchSecurity.com's resources on CISSP certification training Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/ Osborne, 2001, Page 280.

QUESTION 188
The National Institute of Standards and Technology (NIST) standard pertaining to perimeter protection states that critical areas should be illuminated up to?

A. Illiminated at nine feet high with at least three foot-candles

B. Illiminated at eight feet high with at least three foot-candles

C. Illiminated at eight feet high with at least two foot-candles

D. Illuminated at nine feet high with at least two foot-candles

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The National Institute of Standards and Technology (NIST) standard pertaining to perimeter protection states that critical areas should be illuminated eight feet high with at least two foot-candles.
It can also be referred to as illuminating to a height of eight feet, with a BRIGHTNESS of two footcandles. One footcandle 10.764 lux. The footcandle (or lumen per square foot) is a non-SI unit of illuminance. Like the BTU, it is obsolete but it is still in fairly common use in the United States, particularly in construction-related engineering and in building codes. Because lux and footcandles are different units of the same quantity, it is perfectly valid to convert footcandles to lux and vice versa.
The name "footcandle" conveys "the illuminance cast on a surface by a one-candela source one foot away." As natural as this sounds, this style of name is now frowned upon, because the dimensional formula for the unit is not foot · candela, but lumens per square foot. Some sources do however note that the "lux" can be thought of as a "metre-candle" (i.e. the illuminance cast on a surface by a one-candela source one meter away). A source that is farther away casts less illumination than one that is close, so one lux is less illuminance than one footcandle. Since illuminance follows the inverse-square law, and since one foot = 0.3048 m, one lux = 0.30482 footcandle 1/10.764 footcandle.
TIPS FROM CLEMENT:
Illuminance (light level) The amount of light, measured in foot-candles (US unit), that falls n a surface, either horizontal or vertical.
Parking lots lighting needs to be an average of 2 foot candles; uniformity of not more than 3:1, no area less than 1 fc.
All illuminance measurements are to be made on the horizontal plane with a certified light meter calibrated to

NIST standards using traceable light sources.
The CISSP Exam Cram 2 from Michael Gregg says:
Lighting is a commonly used form of perimeter protection. Some studies have found that up to 80% of criminal acts at businesses and shopping centers happen in adjacent parking lots. Therefore, it's easy to see why lighting can be such an important concern.
Outside lighting discourages prowlers and thieves.
The National Institute of Standards and Technologies (NIST) states that, for effective perimeter control, buildings should be illuminated 8 feet high, with 2-foot candle power.
Reference used for this question:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, Page 325.
and
Shon's AIO v5 pg 459
and
http://en.wikipedia.org/wiki/Foot-candle

QUESTION 189
This is a common security issue that is extremely hard to control in large environments. It occurs when a user has more computer rights, permissions, and access than what is required for the tasks the user needs to fulfill. What best describes this scenario?

A. Excessive Rights
B. Excessive Access
C. Excessive Permissions
D. Excessive Privileges

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Even thou all 4 terms are very close to each other, the best choice is Excessive Privileges which would include the other three choices presented.
Reference(s) used for this question:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, Page 645.
and

QUESTION 190
Which of the following are additional access control objectives?

A. Consistency and utility
B. Reliability and utility
C. Usefulness and utility
D. Convenience and utility

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Availability assures that a system's authorized users have timely and uninterrupted access to the information in the system. The additional access control objectives are reliability and utility. These and other related objectives flow from the organizational security policy. This policy is a high-level statement of management intent regarding the control of access to information and the personnel who are authorized to receive that information. Three things that must be considered for the planning and implementation of access control mechanisms are the threats to the system, the system's vulnerability to these threats, and the risk that the threat may materialize Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 32.

QUESTION 191

Logical or technical controls involve the restriction of access to systems and the protection of information. Which of the following statements pertaining to these types of controls is correct?

A. Examples of these types of controls include policies and procedures, security awareness training, background checks, work habit checks but do not include a review of vacation history, and also do not include increased supervision.
B. Examples of these types of controls do not include encryption, smart cards, access lists, and transmission protocols.
C. Examples of these types of controls are encryption, smart cards, access lists, and transmission protocols.
D. Examples of these types of controls include policies and procedures, security awareness training, background checks, work habit checks, a review of vacation history, and increased supervision.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Logical or technical controls involve the restriction of access to systems and the protection of information. Examples of these types of controls are encryption, smart cards, access lists, and transmission protocols.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

QUESTION 192
Controls provide accountability for individuals who are accessing sensitive information. This accountability is accomplished:

A. through access control mechanisms that require identification and authentication and through the audit function.
B. through logical or technical controls involving the restriction of access to systems and the protection of information.
C. through logical or technical controls but not involving the restriction of access to systems and the protection of information.
D. through access control mechanisms that do not require identification and authentication and do not operate through the audit function.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Controls provide accountability for individuals who are accessing sensitive information. This accountability is accomplished through access control mechanisms that require identification and authentication and through the audit function. These controls must be in accordance with and accurately represent the organization's security policy. Assurance procedures ensure that the control mechanisms correctly implement the security policy for the entire life cycle of an information system.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

QUESTION 193
In Discretionary Access Control the subject has authority, within certain limitations,

A. but he is not permitted to specify what objects can be accessible and so we need to get an independent third party to specify what objects can be accessible.
B. to specify what objects can be accessible.
C. to specify on a aggregate basis without understanding what objects can be accessible.
D. to specify in full detail what objects can be accessible.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: With Discretionary Access Control, the subject has authority, within certain limitations, to specify what objects can be accessible. For example, access control lists can be used. This type of access control is used in local, dynamic situations where the subjects must have the discretion to specify what resources certain users are permitted to access.
When a user, within certain limitations, has the right to alter the access control to certain objects, this is termed as user-directed discretionary access control. In some instances, a hybrid approach is used, which combines the features of user-based and identity-based discretionary access control.

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.
and
HARRIS, Shon, All-In-One CISSP Certification Exam Guide 5th Edition, McGraw-Hill/Osborne, 2010, Chapter 4: Access Control (page 210-211).

QUESTION 194
In non-discretionary access control using Role Based Access Control (RBAC), a central authority determines what subjects can have access to certain objects based on the organizational security policy. The access controls may be based on:

A. The societies role in the organization
B. The individual's role in the organization
C. The group-dynamics as they relate to the individual's role in the organization
D. The group-dynamics as they relate to the master-slave role in the organization

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: In Non-Discretionary Access Control, when Role Based Access Control is being used, a central authority determines what subjects can have access to certain objects based on the organizational security policy. The access controls may be based on the individual's role in the organization.
Reference(S) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

QUESTION 195
In an organization where there are frequent personnel changes, non-discretionary access control using Role Based Access Control (RBAC) is useful because:

A. people need not use discretion
B. the access controls are based on the individual's role or title within the organization.
C. the access controls are not based on the individual's role or title within the organization
D. the access controls are often based on the individual's role or title within the organization

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: In an organization where there are frequent personnel changes, non-discretionary access control (also called Role Based Access Control) is useful because the access controls are based on the individual's role or title within the organization. You can easily configure a new employee acces by assigning the user to a role that has been predefine. The user will implicitly inherit the permissions of the role by being a member of that role. These access permissions defined within the role do not need to be changed whenever a new

person takes over the role.
Another type of non-discretionary access control model is the Rule Based Access Control (RBAC or RuBAC) where a global set of rule is uniformly applied to all subjects accessing the resources.
A good example of RuBAC would be a firewall.
This question is a sneaky one, one of the choice has only one added word to it which is often. Reading questions and their choices very carefully is a must for the real exam. Reading it twice if needed is recommended.
Shon Harris in her book list the following ways of managing RBAC:
Role-based access control can be managed in the following ways:
Non-RBAC Users are mapped directly to applications and no roles are used. (No roles being used)
Limited RBAC Users are mapped to multiple roles and mapped directly to other types of applications that do not have role-based access functionality. (A mix of roles for applications that supports roles and explicit access control would be used for applications that do not support roles) Hybrid RBAC Users are mapped to multiapplication roles with only selected rights assigned to those roles.
Full RBAC Users are mapped to enterprise roles. (Roles are used for all access being granted) NIST defines RBAC as:
Security administration can be costly and prone to error because administrators usually specify access control lists for each user on the system individually. With RBAC, security is managed at a level that corresponds closely to the organization's structure. Each user is assigned one or more roles, and each role is assigned one or more privileges that are permitted to users in that role. Security administration with RBAC consists of determining the operations that must be executed by persons in particular jobs, and assigning employees to the proper roles. Complexities introduced by mutually exclusive roles or role hierarchies are handled by the RBAC software, making security administration easier.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 32.
and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition McGraw-Hill.
and
http://csrc.nist.gov/groups/SNS/rbac/

QUESTION 196
Another type of access control is lattice-based access control. In this type of control a lattice model is applied. How is this type of access control concept applied?

A. The pair of elements is the subject and object, and the subject has an upper bound equal or higher than the upper bound of the object being accessed.
B. The pair of elements is the subject and object, and the subject has an upper bound lower then the upper bound of the object being accessed.
C. The pair of elements is the subject and object, and the subject has no special upper or lower bound needed within the lattice.
D. The pair of elements is the subject and object, and the subject has no access rights in relation to an object.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: To apply this concept to access control, the pair of elements is the subject and object, and the subject has to have an upper bound equal or higher than the object being accessed.
WIKIPEDIA has a great explanation as well:
In computer security, lattice-based access control (LBAC) is a complex access control based on the interaction between any combination of objects (such as resources, computers, and applications) and subjects (such as individuals, groups or organizations). In this type of label-based mandatory access control model, a lattice is used to define the levels of security that an object may have and that a subject may have access to. The subject is only allowed to access an object if the security level of the subject is greater than or equal to that of the object.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer

Security, 2001, John Wiley & Sons, Page 34.
and
http://en.wikipedia.org/wiki/Lattice-based_access_control

QUESTION 197
Detective/Technical measures:

A. include intrusion detection systems and automatically-generated violation reports from audit trail information.
B. do not include intrusion detection systems and automatically-generated violation reportsfrom audit trail information.
C. include intrusion detection systems but do not include automatically-generated violation reports from audit trail information.
D. include intrusion detection systems and customised-generated violation reports from audit trail information.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Detective/Technical measures include intrusion detection systems and automatically-generated violation reports from audit trail information. These reports can indicate variations from "normal" operation or detect known signatures of unauthorized access episodes. In order to limit the amount of audit information flagged and reported by automated violation analysis and reporting mechanisms, clipping levels can be set.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 35.

QUESTION 198
Identification and authentication are the keystones of most access control systems. Identification establishes:

A. User accountability for the actions on the system.
B. Top management accountability for the actions on the system.
C. EDP department accountability for the actions of users on the system.
D. Authentication for actions on the system

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Identification and authentication are the keystones of most access control systems. Identification establishes user accountability for the actions on the system. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system. This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users. Once a person has been identified through the user ID or a similar value, she must be authenticated, which means she must prove she is who she says she is. Three general factors can be used for authentication: something a person knows, something a person has, and something a person is. They are also commonly called authentication by knowledge, authentication by ownership, and authentication by characteristic.
For a user to be able to access a resource, he first must prove he is who he claims to be, has the necessary credentials, and has been given the necessary rights or privileges to perform the actions he is requesting. Once these steps are completed successfully, the user can access and use network resources; however, it is necessary to track the user's activities and enforce accountability for his actions.
Identification describes a method of ensuring that a subject (user, program, or process) is the entity it claims to be. Identification can be provided with the use of a username or account number. To be properly authenticated, the subject is usually required to provide a second piece to the credential set. This piece could be a password, passphrase, cryptographic key, personal identification number (PIN), anatomical attribute, or token. These two credential items are compared to information that has been previously stored for this subject.

If these credentials match the stored information, the subject is authenticated. But we are not done yet. Once the subject provides its credentials and is properly identified, the system it is trying to access needs to determine if this subject has been given the necessary rights and privileges to carry out the requested actions. The system will look at some type of access control matrix or compare security labels to verify that this subject may indeed access the requested resource and perform the actions it is attempting. If the system determines that the subject may access the resource, it authorizes the subject.

Although identification, authentication, authorization, and accountability have close and complementary definitions, each has distinct functions that fulfill a specific requirement in the process of access control. A user may be properly identified and authenticated to the network, but he may not have the authorization to access the files on the file server. On the other hand, a user may be authorized to access the files on the file server, but until she is properly identified and authenticated, those resources are out of reach.

Reference(s) used for this question:

Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition: Access Control ((ISC) 2 Press) (Kindle Locations 889-892). Auerbach Publications. Kindle Edition.

and

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 3875- 3878). McGraw-Hill. Kindle Edition.

and

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 3833- 3848). McGraw-Hill. Kindle Edition.

and

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36.

QUESTION 199

Passwords can be required to change monthly, quarterly, or at other intervals:

A. depending on the criticality of the information needing protection
B. depending on the criticality of the information needing protection and the password'sfrequency of use
C. depending on the password's frequency of use
D. not depending on the criticality of the information needing protection but depending on the password's frequency of use

Correct Answer: B

Explanation

Explanation/Reference:

Explanation: Passwords can be compromised and must be protected. In the ideal case, a password should only be used once. The changing of passwords can also fall between these two extremes. Passwords can be required to change monthly, quarterly, or at other intervals, depending on the criticality of the information needing protection and the password's frequency of use. Obviously, the more times a password is used, the more chance there is of it being compromised.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36 & 37.

QUESTION 200

When submitting a passphrase for authentication, the passphrase is converted into ...

A. a virtual password by the system
B. a new passphrase by the system
C. a new passphrase by the encryption technology
D. a real password by the system which can be used forever

Correct Answer: A

Explanation

Explanation/Reference:

Explanation: Passwords can be compromised and must be protected. In the ideal case, a password should only be used once. The changing of passwords can also fall between these two extremes.
Passwords can be required to change monthly, quarterly, or at other intervals, depending on the criticality of the information needing protection and the password's frequency of use. Obviously, the more times a password is used, the more chance there is of it being compromised. It is recommended to use a passphrase instead of a password. A passphrase is more resistant to attacks. The passphrase is converted into a virtual password by the system. Often time the passphrase will exceed the maximum length supported by the system and it must be trucated into a Virtual Password.
Reference(s) used for this question:
http://www.itl.nist.gov/fipspubs/fip112.htm
and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36 & 37.

QUESTION 201
An alternative to using passwords for authentication in logical or technical access control is:

A. manage without passwords
B. biometrics
C. not there
D. use of them for physical access control

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: An alternative to using passwords for authentication in logical or technical access control is biometrics. Biometrics are based on the Type 3 authentication mechanism-something you are.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37.

QUESTION 202
Almost all types of detection permit a system's sensitivity to be increased or decreased during an inspection process. If the system's sensitivity is increased, such as in a biometric authentication system, the system becomes increasingly selective and has the possibility of generating:

A. Lower False Rejection Rate (FRR)
B. Higher False Rejection Rate (FRR)
C. Higher False Acceptance Rate (FAR)
D. It will not affect either FAR or FRR

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Almost all types of detection permit a system's sensitivity to be increased or decreased during an inspection process. If the system's sensitivity is increased, such as in a biometric authentication system, the system becomes increasingly selective and has a higher False Rejection Rate (FRR).
Conversely, if the sensitivity is decreased, the False Acceptance Rate (FRR) will increase. Thus, to have a valid measure of the system performance, the Cross Over Error (CER) rate is used. The Crossover Error Rate (CER) is the point at which the false rejection rates and the false acceptance rates are equal. The lower the value of the CER, the more accurate the system. There are three categories of biometric accuracy measurement (all represented as percentages):
False Reject Rate (a Type I Error): When authorized users are falsely rejected as unidentified or unverified.
False Accept Rate (a Type II Error): When unauthorized persons or imposters are falsely accepted as authentic.
Crossover Error Rate (CER): The point at which the false rejection rates and the false acceptance rates are

equal. The smaller the value of the CER, the more accurate the system.

NOTE:

Within the ISC2 book they make use of the term Accept or Acceptance and also Reject or Rejection when referring to the type of errors within biometrics. Below we make use of Acceptance and Rejection throughout the text for conistency. However, on the real exam you could see either of the terms.

Performance of biometrics

Different metrics can be used to rate the performance of a biometric factor, solution or application. The most common performance metrics are the False Acceptance Rate FAR and the False Rejection Rate FRR.

When using a biometric application for the first time the user needs to enroll to the system. The system requests fingerprints, a voice recording or another biometric factor from the operator, this input is registered in the database as a template which is linked internally to a user ID. The next time when the user wants to authenticate or identify himself, the biometric input provided by the user is compared to the template(s) in the database by a matching algorithm which responds with acceptance (match) or rejection (no match).

FAR and FRR

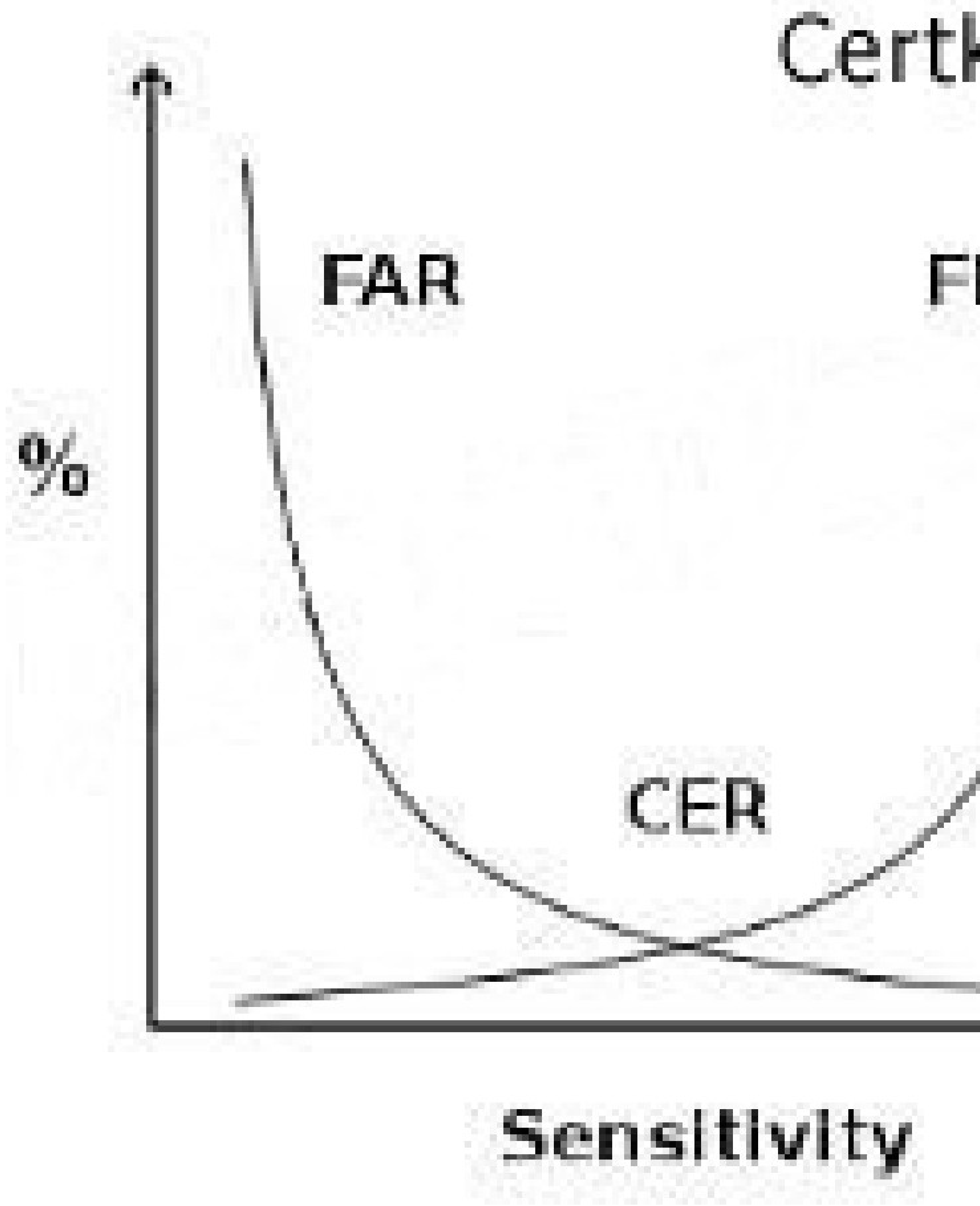
The FAR or False Acceptance rate is the probability that the system incorrectly authorizes a nonauthorized person, due to incorrectly matching the biometric input with a valid template. The FAR is normally expressed as a percentage, following the FAR definition this is the percentage of invalid inputs which are incorrectly accepted.

The FRR or False Rejection Rate is the probability that the system incorrectly rejects access to an authorized person, due to failing to match the biometric input provided by the user with a stored template. The FRR is normally expressed as a percentage, following the FRR definition this is the percentage of valid inputs which are incorrectly rejected. FAR and FRR are very much dependent on the biometric factor that is used and on the technical implementation of the biometric solution. Furthermore the FRR is strongly person dependent, a personal FRR can be determined for each individual.

Take this into account when determining the FRR of a biometric solution, one person is insufficient to establish an overall FRR for a solution. Also FRR might increase due to environmental conditions or incorrect use, for example when using dirty fingers on a fingerprint reader. Mostly the FRR lowers when a user gains more experience in how to use the biometric device or software. FAR and FRR are key metrics for biometric solutions, some biometric devices or software even allow to tune them so that the system more quickly matches or rejects. Both FRR and FAR are important, but for most applications one of them is considered most important. Two examples to illustrate this:

When biometrics are used for logical or physical access control, the objective of the application is to disallow access to unauthorized individuals under all circumstances. It is clear that a very low FAR is needed for such an application, even if it comes at the price of a higher FRR. When surveillance cameras are used to screen a crowd of people for missing children, the objective of the application is to identify any missing children that come up on the screen. When the identification of those children is automated using a face recognition software, this software has to be set up with a low FRR. As such a higher number of matches will be false positives, but these can be reviewed quickly by surveillance personnel. False Acceptance Rate is also called False Match Rate, and False Rejection Rate is sometimes referred to as False Non-Match Rate.

crossover error rate


FAR
%
CER
Sensitivity

Above see a graphical representation of FAR and FRR errors on a graph, indicating the CER CER
The Crossover Error Rate or CER is illustrated on the graph above. It is the rate where both FAR and FRR are equal.
The matching algorithm in a biometric software or device uses a (configurable) threshold which determines how close to a template the input must be for it to be considered a match. This threshold value is in some cases referred to as sensitivity, it is marked on the X axis of the plot. When you reduce this threshold there will be more false acceptance errors (higher FAR) and less false rejection errors (lower FRR), a higher threshold will lead to lower FAR and higher FRR.
Speed
Most manufacturers of biometric devices and softwares can give clear numbers on the time it takes to enroll as well on the time for an individual to be authenticated or identified using their application. If speed is important then take your time to consider this, 5 seconds might seem a short time on paper or when testing a device but if hundreds of people will use the device multiple times a day the cumulative loss of time might be significant.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 2723-2731). Auerbach Publications. Kindle Edition.
and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37.
and
http://www.biometric-solutions.com/index.php?story=performance_biometrics

QUESTION 203
In the context of Biometric authentication, what is a quick way to compare the accuracy of devices. In general, the device that have the lowest value would be the most accurate. Which of the following would be used to compare accuracy of devices?

A. the CER is used.
B. the FRR is used
C. the FAR is used
D. the FER is used

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: equal error rate or crossover error rate (EER or CER): the rate at which both accept and reject errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is most accurate.
In the context of Biometric Authentication almost all types of detection permit a system's sensitivity to be increased or decreased during an inspection process. If the system's sensitivity is increased, such as in an airport metal detector, the system becomes increasingly selective and has a higher False Reject Rate (FRR). Conversely, if the sensitivity is decreased, the False Acceptance Rate (FAR) will increase. Thus, to have a valid measure of the system performance, the CrossOver Error Rate (CER) is used.
The following are used as performance metrics for biometric systems:
false accept rate or false match rate (FAR or FMR): the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted. In case of similarity scale, if the person is imposter in real, but the matching score is higher than the threshold, then he is treated as genuine that increase the FAR and hence performance also depends upon the selection of threshold value. false reject rate or false non-match rate (FRR or FNMR): the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected. failure to enroll rate (FTE or FER): the rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low quality inputs. failure to capture rate (FTC): Within automatic systems, the probability that the system fails to detect a biometric input when presented correctly.
template capacity: the maximum number of sets of data which can be stored in the system.

Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37.
and
Wikipedia at: https://en.wikipedia.org/wiki/Biometrics

QUESTION 204
Because all the secret keys are held and authentication is performed on the Kerberos TGS and the authentication servers, these servers are vulnerable to:

A. neither physical attacks nor attacks from malicious code.
B. physical attacks only
C. both physical attacks and attacks from malicious code.
D. physical attacks but not attacks from malicious code.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Since all the secret keys are held and authentication is performed on the Kerberos TGS and the authentication servers, these servers are vulnerable to both physical attacks and attacks from malicious code. Because a client's password is used in the initiation of the Kerberos request for the service protocol, password guessing can be used to impersonate a client. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 42.

QUESTION 205
The throughput rate is the rate at which individuals, once enrolled, can be processed and identified or authenticated by a biometric system. Acceptable throughput rates are in the range of:

A. 100 subjects per minute.
B. 25 subjects per minute.
C. 10 subjects per minute.
D. 50 subjects per minute.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The throughput rate is the rate at which individuals, once enrolled, can be processed and identified or authenticated by a biometric system. Acceptable throughput rates are in the range of 10 subjects per minute. Things that may impact the throughput rate for some types of biometric systems may include:
A concern with retina scanning systems may be the exchange of body fluids on the eyepiece. Another concern would be the retinal pattern that could reveal changes in a person's health, such as diabetes or high blood pressure.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 38.

QUESTION 206
In addition to the accuracy of the biometric systems, there are other factors that must also be considered:

A. These factors include the enrollment time and the throughput rate, but not acceptability.
B. These factors do not include the enrollment time, the throughput rate, and acceptability.
C. These factors include the enrollment time, the throughput rate, and acceptability.
D. These factors include the enrollment time, but not the throughput rate, neither the acceptability.

Correct Answer: C

Explanation

Explanation/Reference:

Explanation: In addition to the accuracy of the biometric systems, there are other factors that must also be considered.

These factors include the enrollment time, the throughput rate, and acceptability. Enrollment time is the time it takes to initially "register" with a system by providing samples of the biometric characteristic to be evaluated. An acceptable enrollment time is around two minutes. For example, in fingerprint systems, the actual fingerprint is stored and requires approximately 250kb per finger for a high quality image. This level of information is required for one-to-many searches in forensics applications on very large databases. In finger-scan technology, a full fingerprint is not stored-the features extracted from this fingerprint are stored using a small template that requires approximately 500 to 1000 bytes of storage. The original fingerprint cannot be reconstructed from this template. Updates of the enrollment information may be required because some biometric characteristics, such as voice and signature, may change with time.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37 & 38.

QUESTION 207

Which of the following biometric devices has the lowest user acceptance level?

A. Retina Scan

B. Fingerprint scan

C. Hand geometry

D. Signature recognition

Correct Answer: A

Explanation

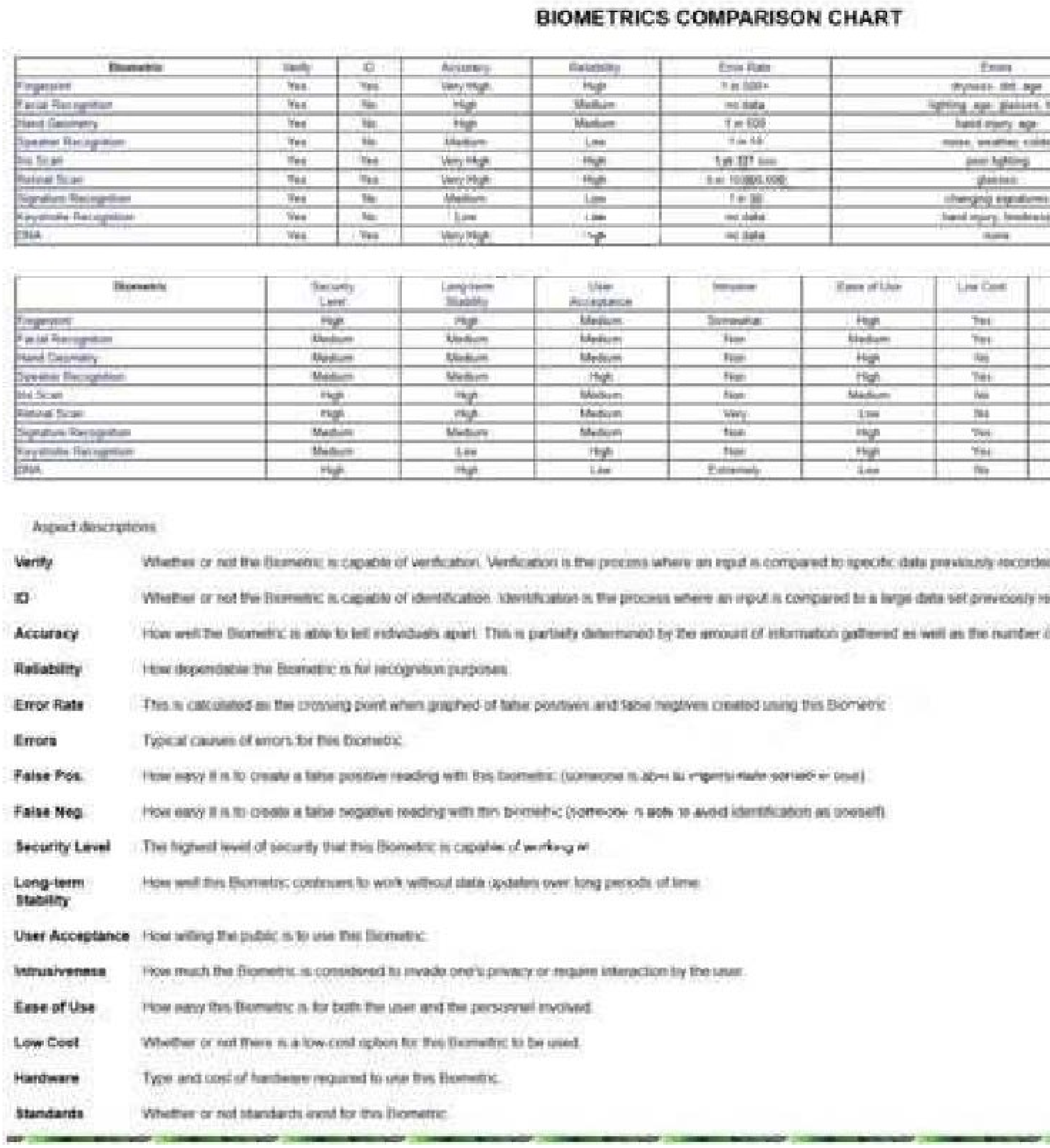
Explanation/Reference:

Explanation: According to the cited reference, of the given options, the Retina scan has the lowest user acceptance level as it is needed for the user to get his eye close to a device and it is not user friendly and very intrusive.

However, retina scan is the most precise with about one error per 10 millions usage. Look at the 2 tables below. If necessary right click on the image and save it on your desktop for a larger view or visit the web site directly at

https://sites.google.com/site/biometricsecuritysolutions/crossover-accuracy .

Biometric Comparison Chart



BIOMETRICS COMPARISON CHART

Biometric	Verify	ID	Accuracy	Reliability	Error Rate	Errors
Fingerprint	Yes	Yes	Very High	High	1 in 500+	dryness, dirt, age
Facial Recognition	Yes	No	High	Medium	no data	lighting, age, glasses, h
Hand Geometry	Yes	No	High	Medium	1 in 500	hand injury, age
Speaker Recognition	Yes	No	Medium	Low	1 in 50	noise, weather, colds
Iris Scan	Yes	Yes	Very High	High	1 in 131,000	poor lighting
Retinal Scan	Yes	Yes	Very High	High	1 in 10,000,000	glasses
Signature Recognition	Yes	No	Medium	Low	1 in 50	changing signatures
Keystroke Recognition	Yes	No	Low	Low	no data	hand injury, tiredness
DNA	Yes	Yes	Very High	High	no data	none

Biometric	Security Level	Long-term Stability	User Acceptance	Intrusive	Ease of Use	Low Cost
Fingerprint	High	High	Medium	Somewhat	High	Yes
Facial Recognition	Medium	Medium	Medium	Non	Medium	Yes
Hand Geometry	Medium	Medium	Medium	Non	High	No
Speaker Recognition	Medium	Medium	High	Non	High	Yes
Iris Scan	High	High	Medium	Non	Medium	No
Retinal Scan	High	High	Medium	Very	Low	No
Signature Recognition	Medium	Medium	Medium	Non	High	Yes
Keystroke Recognition	Medium	Low	High	Non	High	Yes
DNA	High	High	Low	Extremely	Low	No

Aspect descriptions

Verify Whether or not the Biometric is capable of verification. Verification is the process where an input is compared to specific data previously recorde

ID Whether or not the Biometric is capable of identification. Identification is the process where an input is compared to a large data set previously re

Accuracy How well the Biometric is able to tell individuals apart. This is partially determined by the amount of information gathered as well as the number o

Reliability How dependable the Biometric is for recognition purposes.

Error Rate This is calculated as the crossing point when graphed of false positives and false negatives created using this Biometric.

Errors Typical causes of errors for this Biometric.

False Pos. How easy it is to create a false positive reading with this Biometric (someone is able to impersonate someone else).

False Neg. How easy it is to create a false negative reading with this biometric (someone is able to avoid identification as oneself).

Security Level The highest level of security that this Biometric is capable of working at.

Long-term Stability How well this Biometric continues to work without data updates over long periods of time.

User Acceptance How willing the public is to use this Biometric.

Intrusiveness How much the Biometric is considered to invade one's privacy or require interaction by the user.

Ease of Use How easy this Biometric is for both the user and the personnel involved.

Low Cost Whether or not there is a low-cost option for this Biometric to be used.

Hardware Type and cost of hardware required to use this Biometric.

Standards Whether or not standards exist for this Biometric.

Biometric Aspect Descriptions
Reference(s) used for this question:
RHODES, Keith A., Chief Technologist, United States General Accounting Office, National Preparedness, Technologies to Secure Federal Buildings, April 2002 (page 10).

and
https://sites.google.com/site/biometricsecuritysolutions/crossover-accuracy

QUESTION 208
Which of the following would be an example of the best password?

A. golf001
B. Elizabeth
C. T1me4g0lF
D. password

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The best passwords are those that are both easy to remember and hard to crack using a dictionary attack. The best way to create passwords that fulfil both criteria is to use two small unrelated words or phonemes, ideally with upper and lower case characters, a special character, and/or a number. Shouldn't be used: common names, DOB, spouse, phone numbers, words found in dictionaries or system defaults.
Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 1.

QUESTION 209
A network-based vulnerability assessment is a type of test also referred to as:

A. An active vulnerability assessment.
B. A routing vulnerability assessment.
C. A host-based vulnerability assessment.
D. A passive vulnerability assessment.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: A network-based vulnerability assessment tool/system either re-enacts system attacks, noting and recording responses to the attacks, or probes different targets to infer weaknesses from their responses. Since the assessment is actively attacking or scanning targeted systems, network-based vulnerability assessment systems are also called active vulnerability systems.
There are mostly two main types of test:
PASSIVE: You don't send any packet or interact with the remote target. You make use of public database and other techniques to gather information about your target. ACTIVE: You do send packets to your target, you attempt to stimulate response which will help you in gathering information about hosts that are alive, services runnings, port state, and more.
See example below of both types of attacks:
Eavesdropping and sniffing data as it passes over a network are considered passive attacks because the attacker is not affecting the protocol, algorithm, key, message, or any parts of the encryption system. Passive attacks are hard to detect, so in most cases methods are put in place to try to prevent them rather than to detect and stop them. Altering messages , modifying system files, and masquerading as another individual are acts that are considered active attacks because the attacker is actually doing something instead of sitting back and gathering data. Passive attacks are usually used to gain information prior to carrying out an active attack.
IMPORTANT NOTE:
On the commercial vendors will sometimes use different names for different types of scans. However, the exam is product agnostic. They do not use vendor terms but general terms. Experience could trick you into selecting the wrong choice sometimes. See feedback from Jason below:
"I am a system security analyst. It is my daily duty to perform system vulnerability analysis. We use Nessus and Retina (among other tools) to perform our network based vulnerability scanning. Both commercially available tools refer to a network based vulnerability scan as a "credentialed" scan. Without credentials, the scan tool cannot login to the system being scanned, and as such will only receive a port scan to see what ports

are open and exploitable" Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 865). McGraw-Hill. Kindle Edition.
and
DUPUIS, Clement, Access Control Systems and Methodology CISSP Open Study Guide, version 1.0, march 2002 (page 97).

QUESTION 210
Which of the following is NOT a form of detective administrative control?

A. Rotation of duties
B. Required vacations
C. Separation of duties
D. Security reviews and audits

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Detective administrative controls warn of administrative control violations. Rotation of duties, required vacations and security reviews and audits are forms of detective administrative controls. Separation of duties is the practice of dividing the steps in a system function among different individuals, so as to keep a single individual from subverting the process, thus a preventive control rather than a detective control.
Source: DUPUIS, Cl?ment, Access Control Systems and Methodology CISSP Open Study Guide, version 1.0 (march 2002).

QUESTION 211
Which TCSEC level is labeled Controlled Access Protection?

A. C1
B. C2
C. C3
D. B1

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: C2 is labeled Controlled Access Protection. The TCSEC defines four divisions: D, C, B and A where division A has the highest security. Each division represents a significant difference in the trust an individual or organization can place on the evaluated system. Additionally divisions C, B and A are broken into a series of hierarchical subdivisions called classes: C1, C2, B1, B2, B3 and A1. Each division and class expands or modifies as indicated the requirements of the immediately prior division or class.
D -- Minimal protection
Reserved for those systems that have been evaluated but that fail to meet the requirements for a higher division
C -- Discretionary protection
C1 -- Discretionary Security Protection
Identification and authentication
Separation of users and data
Discretionary Access Control (DAC) capable of enforcing access limitations on an individual basis Required System Documentation and user manuals
C2 -- Controlled Access Protection
More finely grained DAC
Individual accountability through login procedures
Audit trails
Object reuse

Resource isolation
B -- Mandatory protection
B1 -- Labeled Security Protection
Informal statement of the security policy model
Data sensitivity labels
Mandatory Access Control (MAC) over selected subjects and objects Label exportation capabilities
All discovered flaws must be removed or otherwise mitigated Design specifications and verification
B2 -- Structured Protection
Security policy model clearly defined and formally documented DAC and MAC enforcement extended to all subjects and objects Covert storage channels are analyzed for occurrence and bandwidth Carefully structured into protection-critical and non-protection-critical elements Design and implementation enable more comprehensive testing and review Authentication mechanisms are strengthened
Trusted facility management is provided with administrator and operator segregation Strict configuration management controls are imposed
B3 -- Security Domains
Satisfies reference monitor requirements
Structured to exclude code not essential to security policy enforcement Significant system engineering directed toward minimizing complexity Security administrator role defined
Audit security-relevant events
Automated imminent intrusion detection, notification, and response Trusted system recovery procedures
Covert timing channels are analyzed for occurrence and bandwidth An example of such a system is the XTS-300, a precursor to the XTS-400 A -- Verified protection
A1 -- Verified Design
Functionally identical to B3
Formal design and verification techniques including a formal top-level specification Formal management and distribution procedures
An example of such a system is Honeywell's Secure Communications Processor SCOMP, a precursor to the XTS-400
Beyond A1
System Architecture demonstrates that the requirements of self-protection and completeness for reference monitors have been implemented in the Trusted Computing Base (TCB). Security Testing automatically generates test-case from the formal top-level specification or formal lower-level specifications.
Formal Specification and Verification is where the TCB is verified down to the source code level, using formal verification methods where feasible.
Trusted Design Environment is where the TCB is designed in a trusted facility with only trusted (cleared) personnel.
The following are incorrect answers:
C1 is Discretionary security
C3 does not exists, it is only a detractor
B1 is called Labeled Security Protection.
Reference(s) used for this question:
HARE, Chris, Security management Practices CISSP Open Study Guide, version 1.0, april 1999.
and
AIOv4 Security Architecture and Design (pages 357 - 361) AIOv5 Security Architecture and Design (pages 358 - 362)

QUESTION 212
Which security model is based on the military classification of data and people with clearances?

A. Brewer-Nash model
B. Clark-Wilson model
C. Bell-LaPadula model
D. Biba model

Correct Answer: C
Explanation

Explanation/Reference:

Explanation: The Bell-LaPadula model is a confidentiality model for information security based on the military classification of data, on people with clearances and data with a classification or sensitivity model. The Biba, Clark-Wilson and Brewer-Nash models are concerned with integrity. Source: HARE, Chris, Security Architecture and Models, Area 6 CISSP Open Study Guide, January 2002.

QUESTION 213
What mechanism automatically causes an alarm originating in a data center to be transmitted over the local municipal fire or police alarm circuits for relaying to both the local police/fire station and the appropriate headquarters?

A. Central station alarm
B. Proprietary alarm
C. A remote station alarm
D. An auxiliary station alarm

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Auxiliary station alarms automatically cause an alarm originating in a data center to be transmitted over the local municipal fire or police alarm circuits for relaying to both the local police/fire station and the appropriate headquarters. They are usually Municipal Fire Alarm Boxes are installed at your business or building, they are wired directly into the fire station. Central station alarms are operated by private security organizations. It is very similar to a proprietary alarm system (see below). However, the biggest difference is the monitoring and receiving of alarm is done off site at a central location manned by non staff members. It is a third party.
Proprietary alarms are similar to central stations alarms except that monitoring is performed directly on the protected property. This type of alarm is usually use to protect large industrials or commercial buildings. Each of the buildings in the same vincinity has their own alarm system, they are all wired together at a central location within one of the building acting as a common receiving point. This point is usually far away from the other building so it is not under the same danger. It is usually man 24 hours a day by a trained team who knows how to react under different conditions. A remote station alarm is a direct connection between the signal-initiating device at the protected property and the signal-receiving device located at a remote station, such as the fire station or usually a monitoring service. This is the most popular type of implementation and the owner of the premise must pay a monthly monitoring fee. This is what most people use in their home where they get a company like ADT to receive the alarms on their behalf. A remote system differs from an auxiliary system in that it does not use the municipal fire of police alarm circuits.
Reference(s) used for this question:
ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 11: Physical Security (page 211).
and
Great presentation J.T.
A. Stone on SlideShare

QUESTION 214
Which of the following does not apply to system-generated passwords?

A. Passwords are harder to remember for users.
B. If the password-generating algorithm gets to be known, the entire system is in jeopardy.
C. Passwords are more vulnerable to brute force and dictionary attacks.
D. Passwords are harder to guess for attackers.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Users tend to choose easier to remember passwords. System-generated passwords can provide stronger, harder to guess passwords. Since they are based on rules provided by the administrator, they can

include combinations of uppercase/lowercase letters, numbers and special characters, making them less vulnerable to brute force and dictionary attacks. One danger is that they are also harder to remember for users, who will tend to write them down, making them more vulnerable to anyone having access to the user's desk. Another danger with system-generated passwords is that if the password-generating algorithm gets to be known, the entire system is in jeopardy.
Source: RUSSEL, Deborah & GANGEMI, G.T. Sr., Computer Security Basics, O'Reilly, July 1992 (page 64).

QUESTION 215
Which of the following is not a preventive login control?

A. Last login message
B. Password aging
C. Minimum password length
D. Account expiration

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The last login message displays the last login date and time, allowing a user to discover if their account was used by someone else. Hence, this is rather a detective control. Source: RUSSEL, Deborah & GANGEMI, G.T. Sr., Computer Security Basics, O'Reilly, July 1992 (page 63).

QUESTION 216
Which of the following forms of authentication would most likely apply a digital signature algorithm to every bit of data that is sent from the claimant to the verifier?

A. Dynamic authentication
B. Continuous authentication
C. Encrypted authentication
D. Robust authentication

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Continuous authentication is a type of authentication that provides protection against impostors who can see, alter, and insert information passed between the claimant and verifier even after the claimant/ verifier authentication is complete. These are typically referred to as active attacks, since they assume that the imposter can actively influence the connection between claimant and verifier. One way to provide this form of authentication is to apply a digital signature algorithm to every bit of data that is sent from the claimant to the verifier. There are other combinations of cryptography that can provide this form of authentication but current strategies rely on applying some type of cryptography to every bit of data sent. Otherwise, any unprotected bit would be suspect. Robust authentication relies on dynamic authentication data that changes with each authenticated session between a claimant and a verifier, but does not provide protection against active attacks. Encrypted authentication is a distracter. Source: GUTTMAN, Barbara & BAGWILL, Robert, NIST Special Publication 800-xx, Internet Security Policy: A Technical Guide, Draft Version, May 25, 2000 (page 34).

QUESTION 217
Who first described the DoD multilevel military security policy in abstract, formal terms?

A. David Bell and Leonard LaPadula
B. Rivest, Shamir and Adleman
C. Whitfield Diffie and Martin Hellman
D. David Clark and David Wilson

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: It was David Bell and Leonard LaPadula who, in 1973, first described the DoD multilevel military security policy in abstract, formal terms. The Bell-LaPadula is a Mandatory Access Control (MAC) model concerned with confidentiality. Rivest, Shamir and Adleman (RSA) developed the RSA encryption algorithm. Whitfield Diffie and Martin Hellman published the Diffie- Hellman key agreement algorithm in 1976. David Clark and David Wilson developed the Clark- Wilson integrity model, more appropriate for security in commercial activities. Source: RUSSEL, Deborah & GANGEMI, G.T. Sr., Computer Security Basics, O'Reilly, July 1992 (pages 78,109).

QUESTION 218
What is the most critical characteristic of a biometric identifying system?

A. Perceived intrusiveness
B. Storage requirements
C. Accuracy
D. Scalability

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Accuracy is the most critical characteristic of a biometric identifying verification system.
Accuracy is measured in terms of false rejection rate (FRR, or type I errors) and false acceptance rate (FAR or type II errors).
The Crossover Error Rate (CER) is the point at which the FRR equals the FAR and has become the most important measure of biometric system accuracy. Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 1, Biometric Identification (page 9).

QUESTION 219
What is considered the most important type of error to avoid for a biometric access control system?

A. Type I Error
B. Type II Error
C. Combined Error Rate
D. Crossover Error Rate

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: When a biometric system is used for access control, the most important error is the false accept or false acceptance rate, or Type II error, where the system would accept an impostor.
A Type I error is known as the false reject or false rejection rate and is not as important in the security context as a type II error rate. A type one is when a valid company employee is rejected by the system and he cannot get access even thou it is a valid user. The Crossover Error Rate (CER) is the point at which the false rejection rate equals the false acceptance rate if your would create a graph of Type I and Type II errors. The lower the CER the better the device would be.
The Combined Error Rate is a distracter and does not exist. Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 1, Biometric Identification (page 10).

QUESTION 220
How can an individual/person best be identified or authenticated to prevent local masquarading attacks?

A. UserId and password
B. Smart card and PIN code
C. Two-factor authentication
D. Biometrics

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The only way to be truly positive in authenticating identity for access is to base the authentication on the physical attributes of the persons themselves (i.e., biometric identification). Physical attributes cannot be shared, borrowed, or duplicated. They ensure that you do identify the person, however they are not perfect and they would have to be supplemented by another factor. Some people are getting thrown off by the term Masquarade. In general, a masquerade is a disguise. In terms of communications security issues, a masquerade is a type of attack where the attacker pretends to be an authorized user of a system in order to gain access to it or to gain greater privileges than they are authorized for. A masquerade may be attempted through the use of stolen logon IDs and passwords, through finding security gaps in programs, or through bypassing the authentication mechanism. Spoofing is another term used to describe this type of attack as well.
A UserId only provides for identification.
A password is a weak authentication mechanism since passwords can be disclosed, shared, written down, and more.
A smart card can be stolen and its corresponding PIN code can be guessed by an intruder. A smartcard can be borrowed by a friend of yours and you would have no clue as to who is really logging in using that smart card.
Any form of two-factor authentication not involving biometrics cannot be as reliable as a biometric system to identify the person.
Biometric identifying verification systems control people. If the person with the correct hand, eye, face, signature, or voice is not present, the identification and verification cannot take place and the desired action (i.e., portal passage, data, or resource access) does not occur. As has been demonstrated many times, adversaries and criminals obtain and successfully use access cards, even those that require the addition of a PIN. This is because these systems control only pieces of plastic (and sometimes information), rather than people. Real asset and resource protection can only be accomplished by people, not cards and information, because unauthorized persons can (and do) obtain the cards and information. Further, life-cycle costs are significantly reduced because no card or PIN administration system or personnel are required. The authorized person does not lose physical characteristics (i.e., hands, face, eyes, signature, or voice), but cards and PINs are continuously lost, stolen, or forgotten. This is why card access systems require systems and people to administer, control, record, and issue (new) cards and PINs. Moreover, the cards are an expensive and recurring cost.
NOTE FROM CLEMENT:
This question has been generating lots of interest. The keyword in the question is: Individual (the person) and also the authenticated portion as well.
I totally agree with you that Two Factors or Strong Authentication would be the strongest means of authentication. However the question is not asking what is the strongest mean of authentication, it is asking what is the best way to identify the user (individual) behind the technology. When answering questions do not make assumptions to facts not presented in the question or answers. Nothing can beat Biometrics in such case. You cannot lend your fingerprint and pin to someone else, you cannot borrow one of my eye balls to defeat the Iris or Retina scan. This is why it is the best method to authenticate the user.
I think the reference is playing with semantics and that makes it a bit confusing. I have improved the question to make it a lot clearer and I have also improve the explanations attached with the question.
The reference mentioned above refers to authenticating the identity for access. So the distinction is being made that there is identity and there is authentication. In the case of physical security the enrollment process is where the identity of the user would be validated and then the biometrics features provided by the user would authenticate the user on a one to one matching basis (for authentication) with the reference contained in the database of biometrics templates. In the case of system access, the user might have to provide a username, a pin, a passphrase, a smart card, and then provide his biometric attributes.
Biometric can also be used for Identification purpose where you do a one to many match. You take a facial scan of someone within an airport and you attempt to match it with a large database of known criminal and

terrorists. This is how you could use biometric for Identification. There are always THREE means of authentication, they are:
Something you know (Type 1)
Something you have (Type 2)
Something you are (Type 3)
Reference(s) used for this question:
TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1) , 2000, CRC Press, Chapter 1, Biometric Identification (page 7).
and
Search Security at http://searchsecurity.techtarget.com/definition/masquerade

QUESTION 221
Which authentication technique best protects against hijacking?

A. Static authentication
B. Continuous authentication
C. Robust authentication
D. Strong authentication

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: A continuous authentication provides protection against impostors who can see, alter, and insert information passed between the claimant and verifier even after the claimant/verifier authentication is complete. This is the best protection against hijacking. Static authentication is the type of authentication provided by traditional password schemes and the strength of the authentication is highly dependent on the difficulty of guessing passwords. The robust authentication mechanism relies on dynamic authentication data that changes with each authenticated session between a claimant and a verifier, and it does not protect against hijacking. Strong authentication refers to a two-factor authentication (like something a user knows and something a user is).
Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 3: Secured Connections to External Networks (page 51).

QUESTION 222
Which of the following is not a security goal for remote access?

A. Reliable authentication of users and systems
B. Protection of confidential data
C. Easy to manage access control to systems and network resources
D. Automated login for remote users

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: An automated login function for remote users would imply a weak authentication, thus certainly not a security goal.
Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition, volume 2, 2001, CRC Press, Chapter 5: An Introduction to Secure Remote Access (page 100).

QUESTION 223
Which of the following questions is less likely to help in assessing identification and authentication controls?

A. Is a current list maintained and approved of authorized users and their access?
B. Are passwords changed at least every ninety days or earlier if needed?

C. Are inactive user identifications disabled after a specified period of time?

D. Is there a process for reporting incidents?

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Identification and authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system. Access control usually requires that the system be able to identify and differentiate among users. Reporting incidents is more related to incident response capability (operational control) than to identification and authentication (technical control).
Source: SWANSON, Marianne, NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001 (Pages A-30 to A-32).

QUESTION 224
Which of the following questions is less likely to help in assessing physical access controls?

A. Does management regularly review the list of persons with physical access to sensitive facilities?

B. Is the operating system configured to prevent circumvention of the security software and application controls?

C. Are keys or other access devices needed to enter the computer room and media library?

D. Are visitors to sensitive areas signed in and escorted?

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Physical security and environmental security are part of operational controls, and are measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. All the questions above are useful in assessing physical access controls except for the one regarding operating system configuration, which is a logical access control.
Source: SWANSON, Marianne, NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001 (Pages A-21 to A-24).

QUESTION 225
Which of the following questions is less likely to help in assessing physical and environmental protection?

A. Are entry codes changed periodically?

B. Are appropriate fire suppression and prevention devices installed and working?

C. Are there processes to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information?

D. Is physical access to data transmission lines controlled?

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Physical security and environmental security are part of operational controls, and are measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. All the questions above are useful in assessing physical and environmental protection except for the one regarding processes that ensuring that unauthorized individuals cannot access information, which is more a production control. Source: SWANSON, Marianne, NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001 (Pages A-21 to A-24).

QUESTION 226
How would nonrepudiation be best classified as?

A. A preventive control

B. A logical control

C. A corrective control

D. A compensating control

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Systems accountability depends on the ability to ensure that senders cannot deny sending information and that receivers cannot deny receiving it. Because the mechanisms implemented in nonrepudiation prevent the ability to successfully repudiate an action, it can be considered as a preventive control.
Source: STONEBURNER, Gary, NIST Special Publication 800-33: Underlying Technical Models for Information Technology Security, National Institute of Standards and Technology, December 2001, page 7.

QUESTION 227
Why should batch files and scripts be stored in a protected area?

A. Because of the least privilege concept.

B. Because they cannot be accessed by operators.

C. Because they may contain credentials.

D. Because of the need-to-know concept.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Because scripts contain credentials, they must be stored in a protected area and the transmission of the scripts must be dealt with carefully. Operators might need access to batch files and scripts. The least privilege concept requires that each subject in a system be granted the most restrictive set of privileges needed for the performance of authorized tasks. The need-to-know principle requires a user having necessity for access to, knowledge of, or possession of specific information required to perform official tasks or services.
Source: WALLHOFF, John, CISSP Summary 2002, April 2002, CBK#1 Access Control System & Methodology (page 3)

QUESTION 228
Which of the following Kerberos components holds all users' and services' cryptographic keys?

A. The Key Distribution Service

B. The Authentication Service

C. The Key Distribution Center

D. The Key Granting Service

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The Key Distribution Center (KDC) holds all users' and services' cryptographic keys. It provides authentication services, as well as key distribution functionality. The Authentication Service is the part of the KDC that authenticates a principal. The Key Distribution Service and Key Granting Service are distracters and are not defined Kerberos components. Source: WALLHOFF, John, CISSP Summary 2002, April 2002, CBK#1 Access Control System & Methodology (page 3)

QUESTION 229

Sensitivity labels are an example of what application control type?

A. Preventive security controls
B. Detective security controls
C. Compensating administrative controls
D. Preventive accuracy controls

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Sensitivity labels are a preventive security application controls, such as are firewalls, reference monitors, traffic padding, encryption, data classification, one-time passwords, contingency planning, separation of development, application and test environments.
The incorrect answers are:
Detective security controls - Intrusion detection systems (IDS), monitoring activities, and audit trails.
Compensating administrative controls - There no such application control. Preventive accuracy controls - data checks, forms, custom screens, validity checks, contingency planning, and backups.
Sources:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 264).
KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter 7: Application Controls, Figure 7.1 (page 360).

QUESTION 230
Which integrity model defines a constrained data item, an integrity verification procedure and a transformation procedure?

A. The Take-Grant model
B. The Biba integrity model
C. The Clark Wilson integrity model
D. The Bell-LaPadula integrity model

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The Clark Wilson integrity model addresses the three following integrity goals: 1) data is protected from modification by unauthorized users; 2) data is protected from unauthorized modification by authorized users; and 3) data is internally and externally consistent. It also defines a Constrained Data Item (CDI), an Integrity Verification Procedure (IVP), a Transformation Procedure (TP) and an Unconstrained Data item. The Bell-LaPadula and Take-Grant models are not integrity models.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architecture and Models (page 205).

QUESTION 231
How should a doorway of a manned facility with automatic locks be configured?

A. It should be configured to be fail-secure.
B. It should be configured to be fail-safe.
C. It should have a door delay cipher lock.
D. It should not allow piggybacking.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Access controls are meant to protect facilities and computers as well as people. In some situations, the objectives of physical access controls and the protection of people's lives may come into conflict. In theses situations, a person's life always takes precedence. Many physical security controls make entry into and out of a facility hard, if not impossible. However, special consideration needs to be taken when this could affect lives. In an information processing facility, different types of locks can be used and piggybacking should be prevented, but the issue here with automatic locks is that they can either be configured as fail-safe or fail-secure. Since there should only be one access door to an information processing facility, the automatic lock to the only door to a man-operated room must be configured to allow people out in case of emergency, hence to be fail-safe (sometimes called fail-open), meaning that upon fire alarm activation or electric power failure, the locking device unlocks. This is because the solenoid that maintains power to the lock to keep it in a locked state fails and thus opens or unlocks the electronic lock.
Fail Secure works just the other way. The lock device is in a locked or secure state with no power applied. Upon authorized entry, a solinoid unlocks the lock temporarily. Thus in a Fail Secure lock, loss of power of fire alarm activation causes the lock to remain in a secure mode.
Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 451). McGraw-Hill.
Kindle Edition.
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 20249-20251). Auerbach Publications. Kindle Edition.

QUESTION 232
Which of following is not a service provided by AAA servers (Radius, TACACS and DIAMETER)?

A. Authentication
B. Administration
C. Accounting
D. Authorization

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Radius, TACACS and DIAMETER are classified as authentication, authorization, and accounting (AAA) servers.
Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Page 33.
also see:
The term "AAA" is often used, describing cornerstone concepts [of the AIC triad] Authentication, Authorization, and Accountability. Left out of the AAA acronym is Identification which is required before the three "A's" can follow. Identity is a claim, Authentication proves an identity, Authorization describes the action you can perform on a system once you have been identified and authenticated, and accountability holds users accountable for their actions. CISSP Study Guide, Conrad Misenar, Feldman p. 10-11, (c) 2010 Elsevier.

QUESTION 233
In response to Access-request from a client such as a Network Access Server (NAS), which of the following is not one of the response from a RADIUS Server?

A. Access-Accept
B. Access-Reject
C. Access-Granted
D. Access-Challenge

Correct Answer: C
Explanation

Explanation/Reference:

Explanation: In response to an access-request from a client, a RADIUS server returns one of three authentication responses: access-accept, access-reject, or access-challenge, the latter being a request for additional authentication information such as a one-time password from a token or a callback identifier.
Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, page 36.

QUESTION 234

Which of the following statements pertaining to RADIUS is incorrect:

A. A RADIUS server can act as a proxy server, forwarding client requests to other authentication domains.
B. Most of RADIUS clients have a capability to query secondary RADIUS servers for redundancy.
C. Most RADIUS servers have built-in database connectivity for billing and reporting purposes.
D. Most RADIUS servers can work with DIAMETER servers.

Correct Answer: D
Explanation

Explanation/Reference:

Explanation: This is the correct answer because it is FALSE. Diameter is an AAA protocol, AAA stands for authentication, authorization and accounting protocol for computer networks, and it is a successor to RADIUS. The name is a pun on the RADIUS protocol, which is the predecessor (a diameter is twice the radius).
The main differences are as follows:
Reliable transport protocols (TCP or SCTP, not UDP)
The IETF is in the process of standardizing TCP Transport for RADIUS Network or transport layer security (IPsec or TLS)
The IETF is in the process of standardizing Transport Layer Security for RADIUS Transition support for RADIUS, although Diameter is not fully compatible with RADIUS Larger address space for attribute-value pairs (AVPs) and identifiers (32 bits instead of 8 bits) Clientserver protocol, with exception of supporting some server-initiated messages as well Both stateful and stateless models can be used
Dynamic discovery of peers (using DNS SRV and NAPTR)
Capability negotiation
Supports application layer acknowledgements, defines failover methods and state machines (RFC 3539)
Error notification
Better roaming support
More easily extended; new commands and attributes can be defined Aligned on 32-bit boundaries
Basic support for user-sessions and accounting
A Diameter Application is not a software application, but a protocol based on the Diameter base protocol (defined in RFC 3588). Each application is defined by an application identifier and can add new command codes and/or new mandatory AVPs. Adding a new optional AVP does not require a new application.
Examples of Diameter applications:
Diameter Mobile IPv4 Application (MobileIP, RFC 4004)
Diameter Network Access Server Application (NASREQ, RFC 4005) Diameter Extensible Authentication Protocol (EAP) Application (RFC 4072) Diameter Credit-Control Application (DCCA, RFC 4006)
Diameter Session Initiation Protocol Application (RFC 4740) Various applications in the 3GPP IP Multimedia Subsystem All of the other choices presented are true. So Diameter is backwork compatible with Radius (to some extent) but the opposite is false.
Reference(s) used for this question:
TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Page 38.
and
https://secure.wikimedia.org/wikipedia/en/wiki/Diameter_%28protocol%29

QUESTION 235

Which of the following is used by RADIUS for communication between clients and servers?

A. TCP
B. SSL

C. UDP

D. SSH

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Page 33.

QUESTION 236
Which of the following protocol was used by the INITIAL version of the Terminal Access Controller Access Control System TACACS for communication between clients and servers?

A. TCP

B. SSL

C. UDP

D. SSH

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The original TACACS, developed in the early ARPANet days, had very limited functionality and used the UDP transport. In the early 1990s, the protocol was extended to include additional functionality and the transport changed to TCP. TACACS is defined in RFC 1492, and uses (either TCP or UDP) port 49 by default. TACACS allows a client to accept a username and password and send a query to a TACACS authentication server, sometimes called a TACACS daemon or simply TACACSD. TACACSD uses TCP and usually runs on port 49. It would determine whether to accept or deny the authentication request and send a response back.
TACACS+
TACACS+ and RADIUS have generally replaced TACACS and XTACACS in more recently built or updated networks. TACACS+ is an entirely new protocol and is not compatible with TACACS or XTACACS. TACACS+ uses the Transmission Control Protocol (TCP) and RADIUS uses the User Datagram Protocol (UDP). Since TCP is connection oriented protocol, TACACS+ does not have to implement transmission control. RADIUS, however, does have to detect and correct transmission errors like packet loss, timeout etc. since it rides on UDP which is connectionless. RADIUS encrypts only the users' password as it travels from the RADIUS client to RADIUS server. All other information such as the username, authorization, accounting are transmitted in clear text. Therefore it is vulnerable to different types of attacks. TACACS+ encrypts all the information mentioned above and therefore does not have the vulnerabilities present in the RADIUS protocol. RADIUS and TACACS + are client/ server protocols, which means the server portion cannot send unsolicited commands to the client portion. The server portion can only speak when spoken to. Diameter is a peer-based protocol that allows either end to initiate communication. This functionality allows the Diameter server to send a message to the access server to request the user to provide another authentication credential if she is attempting to access a secure resource.
Reference(s) used for this question:
http://en.wikipedia.org/wiki/TACACS
and
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 239). McGraw-Hill. Kindle Edition.

QUESTION 237
Which of the following can best eliminate dial-up access through a Remote Access Server as a hacking vector?

A. Using a TACACS+ server.

B. Installing the Remote Access Server outside the firewall and forcing legitimate users to authenticate to the firewall.

C. Setting modem ring count to at least 5.

D. Only attaching modems to non-networked hosts.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Containing the dial-up problem is conceptually easy: by installing the Remote Access Server outside the firewall and forcing legitimate users to authenticate to the firewall, any access to internal resources through the RAS can be filtered as would any other connection coming from the Internet.
The use of a TACACS+ Server by itself cannot eliminate hacking. Setting a modem ring count to 5 may help in defeating war-dialing hackers who look for modem by dialing long series of numbers.
Attaching modems only to non-networked hosts is not practical and would not prevent these hosts from being hacked.
Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 2:
Hackers.

QUESTION 238
In the Bell-LaPadula model, the Star-property is also called:

A. The simple security property

B. The confidentiality property

C. The confinement property

D. The tranquility property

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The Bell-LaPadula model focuses on data confidentiality and access to classified information, in contrast to the Biba Integrity Model which describes rules for the protection of data integrity.
In this formal model, the entities in an information system are divided into subjects and objects. The notion of a "secure state" is defined, and it is proven that each state transition preserves security by moving from secure state to secure state, thereby proving that the system satisfies the security objectives of the model.
The Bell-LaPadula model is built on the concept of a state machine with a set of allowable states in a system. The transition from one state to another state is defined by transition functions. A system state is defined to be "secure" if the only permitted access modes of subjects to objects are in accordance with a security policy.
To determine whether a specific access mode is allowed, the clearance of a subject is compared to the classification of the object (more precisely, to the combination of classification and set of compartments, making up the security level) to determine if the subject is authorized for the specific access mode.
The clearance/classification scheme is expressed in terms of a lattice. The model defines two mandatory access control (MAC) rules and one discretionary access control (DAC) rule with three security properties:
The Simple Security Property - a subject at a given security level may not read an object at a higher security level (no read-up).
The property (read "star"-property) - a subject at a given security level must not write to any object at a lower security level (no write-down). The property is also known as the Confinement property. The Discretionary Security Property - use an access control matrix to specify the discretionary access control.
The transfer of information from a high-sensitivity document to a lower-sensitivity document may happen in the Bell-LaPadula model via the concept of trusted subjects. Trusted Subjects are not restricted by the property. Untrusted subjects are.
Trusted Subjects must be shown to be trustworthy with regard to the security policy. This security model is directed toward access control and is characterized by the phrase: "no read up, no write down." Compare the Biba model, the Clark-Wilson model and the Chinese Wall. With Bell-LaPadula, users can create content only at or above their own security level (i.e. secret researchers can create secret or top-secret files but may not create public files; no write-down). Conversely, users can view content only at or below their own security level (i.e. secret researchers can view public or secret files, but may not view top-secret files; no read-up).

Strong Property
The Strong Property is an alternative to the Property in which subjects may write to objects with only a matching security level. Thus, the write-up operation permitted in the usual Property is not present, only a write-to-same level operation. The Strong Property is usually discussed in the context of multilevel database management systems and is motivated by integrity concerns.
Tranquility principle
The tranquility principle of the Bell-LaPadula model states that the classification of a subject or object does not change while it is being referenced. There are two forms to the tranquility principle:
the "principle of strong tranquility" states that security levels do not change during the normal operation of the system and the "principle of weak tranquility" states that security levels do not change in a way that violates the rules of a given security policy. Another interpretation of the tranquility principles is that they both apply only to the period of time during which an operation involving an object or subject is occurring. That is, the strong tranquility principle means that an object's security level/label will not change during an operation (such as read or write); the weak tranquility principle means that an object's security level/label may change in a way that does not violate the security policy during an operation.
Reference(s) used for this question:
http://en.wikipedia.org/wiki/Biba_Model
http://en.wikipedia.org/wiki/Mandatory_access_control
http://en.wikipedia.org/wiki/Discretionary_access_control http://en.wikipedia.org/wiki/Clark-Wilson_model
http://en.wikipedia.org/wiki/Brewer_and_Nash_model

QUESTION 239
An attack initiated by an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization is known as a(n):

A. active attack
B. outside attack
C. inside attack
D. passive attack

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: An inside attack is an attack initiated by an entity inside the security perimeter, an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization whereas an outside attack is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system. An active attack attempts to alter system resources to affect their operation and a passive attack attempts to learn or make use of the information from the system but does not affect system resources. Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 240
Which of the following can be defined as a framework that supports multiple, optional authentication mechanisms for PPP, including cleartext passwords, challenge-response, and arbitrary dialog sequences?

A. Extensible Authentication Protocol
B. Challenge Handshake Authentication Protocol
C. Remote Authentication Dial-In User Service
D. Multilevel Authentication Protocol.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: RFC 2828 (Internet Security Glossary) defines the Extensible Authentication Protocol as a framework that supports multiple, optional authentication mechanisms for PPP, including cleartext passwords, challenge-response, and arbitrary dialog sequences. It is intended for use primarily by a host or router that

connects to a PPP network server via switched circuits or dial-up lines. The Remote Authentication Dial-In User Service (RADIUS) is defined as an Internet protocol for carrying dial-in user's authentication information and configuration information between a shared, centralized authentication server and a network access server that needs to authenticate the users of its network access ports. The other option is a distracter.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 241
What is a common problem when using vibration detection devices for perimeter control?

A. They are vulnerable to non-adversarial disturbances.
B. They can be defeated by electronic means.
C. Signal amplitude is affected by weather conditions.
D. They must be buried below the frost line.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Vibration sensors are similar and are also implemented to detect forced entry. Financial institutions may choose to implement these types of sensors on exterior walls, where bank robbers may attempt to drive a vehicle through. They are also commonly used around the ceiling and flooring of vaults to detect someone trying to make an unauthorized bank withdrawal. Such sensors are proned to false positive. If there is a large truck with heavy equipment driving by it may trigger the sensor. The same with a storm with thunder and lighting, it may trigger the alarm even thou there are no adversarial threat or disturbance.
The following are incorrect answers:
All of the other choices are incorrect.
Reference used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (pp. 495-496). McGraw-Hill . Kindle Edition.

QUESTION 242
Which of the following security controls might force an operator into collusion with personnel assigned organizationally within a different function in order to gain access to unauthorized data?

A. Limiting the local access of operations personnel
B. Job rotation of operations personnel
C. Management monitoring of audit logs
D. Enforcing regular password changes

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The questions specifically said: "within a different function" which eliminate Job Rotation as a choice.
Management monitoring of audit logs is a detective control and it would not prevent collusion. Changing passwords regularly would not prevent such attack. This question validates if you understand the concept of separation of duties and least privilege. By having operators that have only the minimum access level they need and only what they need to do their duties within a company, the operations personnel would be force to use collusion to defeat those security mechanism.
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 243
What is the name of the first mathematical model of a multi-level security policy used to define the concept of a secure state, the modes of access, and rules for granting access?

A. Clark and Wilson Model

B. Harrison-Ruzzo-Ullman Model
C. Rivest and Shamir Model
D. Bell-LaPadula Model

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 244
Which of the following models does NOT include data integrity or conflict of interest?

A. Biba
B. Clark-Wilson
C. Bell-LaPadula
D. Brewer-Nash

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Bell LaPadula model (Bell 1975): The granularity of objects and subjects is not predefined, but the model prescribes simple access rights. Based on simple access restrictions the Bell LaPadula model enforces a discretionary access control policy enhanced with mandatory rules. Applications with rigid confidentiality requirements and without strong integrity requirements may properly be modeled.
These simple rights combined with the mandatory rules of the policy considerably restrict the spectrum of applications which can be appropriately modeled. Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.
Also check:
Proceedings of the IFIP TC11 12th International Conference on Information Security, Samos (Greece), May 1996, On Security Models.

QUESTION 245
What is the PRIMARY use of a password?

A. Allow access to files.
B. Identify the user.
C. Authenticate the user.
D. Segregate various user's accesses.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 246
The three classic ways of authenticating yourself to the computer security software are: something you know, something you have, and something:

A. you need.
B. you read.
C. you are.
D. you do.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 247
An access system that grants users only those rights necessary for them to perform their work is operating on which security principle?

A. Discretionary Access
B. Least Privilege
C. Mandatory Access
D. Separation of Duties

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 248
Pin, Password, Passphrases, Tokens, smart cards, and biometric devices are all items that can be used for Authentication. When one of these item listed above in conjunction with a second factor to validate authentication, it provides robust authentication of the individual by practicing which of the following?

A. Multi-party authentication
B. Two-factor authentication
C. Mandatory authentication
D. Discretionary authentication

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Once an identity is established it must be authenticated. There exist numerous technologies and implementation of authentication methods however they almost all fall under three major areas.
There are three fundamental types of authentication:
Authentication by knowledge--something a person knows
Authentication by possession--something a person has
Authentication by characteristic--something a person is Logical controls related to these types are called "factors." Something you know can be a password or PIN, something you have can be a token fob or smart card, and something you are is usually some form of biometrics. Single-factor authentication is the employment of one of these factors, two-factor authentication is using two of the three factors, and three-factor authentication is the combination of all three factors.
The general term for the use of more than one factor during authentication is multifactor authentication or strong authentication.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 2367-2379). Auerbach Publications. Kindle Edition.

QUESTION 249
What is one disadvantage of content-dependent protection of information?

A. It increases processing overhead.

B. It requires additional password entry.
C. It exposes the system to data locking.
D. It limits the user's individual address space.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 250
Which of the following is most appropriate to notify an internal user that session monitoring is being conducted?

A. Logon Banners
B. Wall poster
C. Employee Handbook
D. Written agreement

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: This is a tricky question, the keyword in the question is Internal users. There are two possible answers based on how the question is presented, this question could either apply to internal users or ANY anonymous/external users. Internal users should always have a written agreement first, then logon banners serve as a constant reminder.
Banners at the log-on time should be used to notify external users of any monitoring that is being conducted. A good banner will give you a better legal stand and also makes it obvious the user was warned about who should access the system, who is authorized and unauthorized, and if it is an unauthorized user then he is fully aware of trespassing. Anonymous/External users, such as those logging into a web site, ftp server or even a mail server; their only notification system is the use of a logon banner.
References used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 50.
and
Shon Harris, CISSP All-in-one, 5th edition, pg 873

QUESTION 251
What mechanism does a system use to compare the security labels of a subject and an object?

A. Validation Module.
B. Reference Monitor.
C. Clearance Check.
D. Security Module.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Because the Reference Monitor is responsible for access control to the objects by the subjects it compares the security labels of a subject and an object. According to the OIG: The reference monitor is an access control concept referring to an abstract machine that mediates all accesses to objects by subjects based on information in an access control database. The reference monitor must mediate all access, be protected from modification, be verifiable as correct, and must always be invoked. The reference monitor, in accordance with the security policy, controls the checks that are made in the access control database.

The following are incorrect:
Validation Module. A Validation Module is typically found in application source code and is used to validate data being inputted.
Clearance Check. Is a distractor, there is no such thing other than what someone would do when checking if someone is authorized to access a secure facility. Security Module. Is typically a general purpose module that prerforms a variety of security related functions.

OIG CBK, Security Architecture and Design (page 324)
AIO, 4th Edition, Security Architecture and Design, pp 328-328. Wikipedia - http://en.wikipedia.org/wiki/Reference_monitor

QUESTION 252
As per the Orange Book, what are two types of system assurance?

A. Operational Assurance and Architectural Assurance.
B. Design Assurance and Implementation Assurance.
C. Architectural Assurance and Implementation Assurance.
D. Operational Assurance and Life-Cycle Assurance.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Are the two types of assurance mentioned in the Orange book.
The following answers are incorrect:
Operational Assurance and Architectural Assurance. Is incorrect because Architectural Assurance is not a type of assurance mentioned in the Orange book. Design Assurance and Implementation Assurance. Is incorrect because neither are types of assurance mentioned in the Orange book.
Architectural Assurance and Implementation Assurance. Is incorrect because neither are types of assurance mentioned in the Orange book.

QUESTION 253
Which of the following are required for Life-Cycle Assurance?

A. System Architecture and Design specification.
B. Security Testing and Covert Channel Analysis.
C. Security Testing and Trusted distribution.
D. Configuration Management and Trusted Facility Management.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Security testing and trusted distribution are required for Life-Cycle Assurance.
The following answers are incorrect:
System Architecture and Design specification. Is incorrect because System Architecture is not requried for Life-Cycle Assurance.
Security Testing and Covert Channel Analysis. Is incorrect because Covert Channel Analysis is not requried for Life-Cycle Assurance.
Configuration Management and Trusted Facility Management. Is incorrect because Trusted Facility Management. is not requried for Life-Cycle Assurance.

QUESTION 254
Memory management in TCSEC levels B3 and A1 operating systems may utilize "data hiding".
What does this mean?

A. System functions are layered, and none of the functions in a given layer can access data outside that layer.

B. Auditing processes and their memory addresses cannot be accessed by user processes.

C. Only security processes are allowed to write to ring zero memory.

D. It is a form of strong encryption cipher.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Data Hiding is protecting data so that it is only available to higher levels this is done and is also performed by layering, when the software in each layer maintains its own global data and does not directly reference data outside its layers.
The following answers are incorrect:
Auditing processes and their memory addresses cannot be accessed by user processes. Is incorrect because this does not offer data hiding.
Only security processes are allowed to write to ring zero memory. This is incorrect, the security kernel would be responsible for this.
It is a form of strong encryption cipher. Is incorrect because this does not conform to the definition of data hiding.

QUESTION 255
What does "System Integrity" mean?

A. The software of the system has been implemented as designed.

B. Users can't tamper with processes they do not own.

C. Hardware and firmware have undergone periodic testing to verify that they are functioning properly.

D. Design specifications have been verified against the formal top-level specification.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: System Integrity means that all components of the system cannot be tampered with by unauthorized personnel and can be verified that they work properly.
The following answers are incorrect:
The software of the system has been implemented as designed. Is incorrect because this would fall under Trusted system distribution.
Users can't tamper with processes they do not own. Is incorrect because this would fall under Configuration Management.
Design specifications have been verified against the formal top-level specification. Is incorrect because this would fall under Specification and verification.

AIOv3 Security Models and Architecture (pages 302 - 306) DOD TCSEC - http://www.cerberussystems.com/INFOSEC/stds/d520028.htm

QUESTION 256
The Orange Book states that "Hardware and software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB [Trusted Computing Base]." This statement is the formal requirement for:

A. Security Testing.

B. Design Verification.

C. System Integrity.

D. System Architecture Specification.

Correct Answer: C
Explanation

Explanation/Reference:

Explanation: This is a requirement starting as low as C1 within the TCSEC rating. The Orange book requires the following for System Integrity Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.
NOTE FROM CLEMENT:
This is a question that confuses a lot of people because most people take for granted that the orange book with its associated Bell LaPadula model has nothing to do with integrity. However you have to be careful about the context in which the word integrity is being used. You can have Data Integrity and you can have System Integrity which are two completely different things. Yes, the Orange Book does not specifically address the Integrity requirements, however it has to run on top of systems that must meet some integrity requirements.
This is part of what they call operational assurance which is defined as a level of confidence of a trusted system's architecture and implementation that enforces the system's security policy. It includes:
System architecture
Covert channel analysis
System integrity
Trusted recovery
DATA INTEGRITY
Data Integrity is very different from System Integrity. When you have integrity of the data, there are three goals:
1. Prevent authorized users from making unauthorized modifications
2. Preven unauthorized users from making modifications
3. Maintaining internal and external consistancy of the data Bell LaPadula which is based on the Orange Book address does not address Integrity, it addresses only Confidentiality.
Biba address only the first goal of integrity.
Clark-Wilson addresses the three goals of integrity.
In the case of this question, there is a system integrity requirement within the TCB. As mentioned above here is an extract of the requirements: Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.
The following answers are incorrect:
Security Testing. Is incorrect because Security Testing has no set of requirements in the Orange book.
Design Verification. Is incorrect because the Orange book's requirements for Design Verification include: A formal model of the security policy must be clearly identified and documented, including a mathematical proof that the model is consistent with its axioms and is sufficient to support the security policy.
System Architecture Specification. Is incorrect because there are no requirements for System Architecture Specification in the Orange book.
The following reference(s) were used for this question:
Trusted Computer Security Evaluation Criteria (TCSEC), DoD 5200.28-STD, page 15, 18, 25, 31, 40, 50.
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition, Security Architecture and Design, Page 392-397, for users with the Kindle Version see Kindle Locations 28504-28505.
and
DOD TCSEC - http://www.cerberussystems.com/INFOSEC/stds/d520028.htm

QUESTION 257

Which of the following can be used as a covert channel?

A. Storage and timing.
B. Storage and low bits.
C. Storage and permissions.
D. Storage and classification.

Correct Answer: A
Explanation

Explanation/Reference:

Explanation: The Orange book requires protection against two types of covert channels, Timing and Storage.
The following answers are incorrect:
Storage and low bits. Is incorrect because, low bits would not be considered a covert channel. Storage and permissions. Is incorrect because, permissions would not be considered a covert channel.

Storage and classification. Is incorrect because, classification would not be considered a covert channel.

QUESTION 258
Configuration Management controls what?

A. Auditing of changes to the Trusted Computing Base.
B. Control of changes to the Trusted Computing Base.
C. Changes in the configuration access to the Trusted Computing Base.
D. Auditing and controlling any changes to the Trusted Computing Base.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: All of these are components of Configuration Management.
The following answers are incorrect:
Auditing of changes to the Trusted Computing Base. Is incorrect because it refers only to auditing the changes, but nothing about controlling them.
Control of changes to the Trusted Computing Base. Is incorrect because it refers only to controlling the changes, but nothing about ensuring the changes will not lead to a weakness or fault in the system.
Changes in the configuration access to the Trusted Computing Base. Is incorrect because this does not refer to controlling the changes or ensuring the changes will not lead to a weakness or fault in the system.

QUESTION 259
Which of the following exemplifies proper separation of duties?

A. Operators are not permitted modify the system time.
B. Programmers are permitted to use the system console.
C. Console operators are permitted to mount tapes and disks.
D. Tape operators are permitted to use the system console.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: This is an example of Separation of Duties because operators are prevented from modifying the system time which could lead to fraud. Tasks of this nature should be performed by they system administrators.
AIO defines Separation of Duties as a security principle that splits up a critical task among two or more individuals to ensure that one person cannot complete a risky task by himself.
The following answers are incorrect:
Programmers are permitted to use the system console. Is incorrect because programmers should not be permitted to use the system console, this task should be performed by operators. Allowing programmers access to the system console could allow fraud to occur so this is not an example of Separation of Duties..
Console operators are permitted to mount tapes and disks. Is incorrect because operators should be able to mount tapes and disks so this is not an example of Separation of Duties. Tape operators are permitted to use the system console. Is incorrect because operators should be able to use the system console so this is not an example of Separation of Duties.

OIG CBK Access Control (page 98 - 101)
AIOv3 Access Control (page 182)

QUESTION 260
The control of communications test equipment should be clearly addressed by security policy for which of the following reasons?

A. Test equipment is easily damaged.

B. Test equipment can be used to browse information passing on a network.

C. Test equipment is difficult to replace if lost or stolen.

D. Test equipment must always be available for the maintenance personnel.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Test equipment must be secured. There are equipment and other tools that if in the wrong hands could be used to "sniff" network traffic and also be used to commit fraud. The storage and use of this equipment should be detailed in the security policy for this reason.
The following answers are incorrect:
Test equipment is easily damaged. Is incorrect because it is not the best answer, and from a security point of view not relevent.
Test equipment is difficult to replace if lost or stolen. Is incorrect because it is not the best answer, and from a security point of view not relevent.
Test equipment must always be available for the maintenance personnel. Is incorrect because it is not the best answer, and from a security point of view not relevent.

OIG CBK Operations Security (pages 642 - 643)

QUESTION 261
Who is ultimately responsible for the security of computer based information systems within an organization?

A. The tech support team

B. The Operation Team.

C. The management team.

D. The training team.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: If there is no support by management to implement, execute, and enforce security policies and procedure, then they won't work. Senior management must be involved in this because they have an obligation to the organization to protect the assests . The requirement here is for management to show "due diligence" in establishing an effective compliance, or security program.
The following answers are incorrect:
The tech support team. Is incorrect because the ultimate responsibility is with management for the security of computer-based information systems.
The Operation Team. Is incorrect because the ultimate responsibility is with management for the security of computer-based information systems.
The Training Team. Is incorrect because the ultimate responsibility is with management for the security of computer-based information systems.
Reference(s) used for this question:
OIG CBK Information Security Management and Risk Management (page 20 - 22)

QUESTION 262
The major objective of system configuration management is which of the following?

A. system maintenance.

B. system stability.

C. system operations.

D. system tracking.

Correct Answer: B

Explanation

Explanation/Reference:
Explanation: A major objective with Configuration Management is stability. The changes to the system are controlled so that they don't lead to weaknesses or faults in th system.
The following answers are incorrect:
system maintenance. Is incorrect because it is not the best answer. Configuration Management does control the changes to the system but it is not as important as the overall stability of the system.
system operations. Is incorrect because it is not the best answer, the overall stability of the system is much more important.
system tracking. Is incorrect because while tracking changes is important, it is not the best answer. The overall stability of the system is much more important.

QUESTION 263
Which must bear the primary responsibility for determining the level of protection needed for information systems resources?

A. IS security specialists
B. Senior Management
C. Senior security analysts
D. systems Auditors

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: If there is no support by senior management to implement, execute, and enforce security policies and procedure, then they won't work. Senior management must be involved in this because they have an obligation to the organization to protect the assests . The requirement here is for management to show "due diligence" in establishing an effective compliance, or security program. It is senior management that could face legal repercussions if they do not have sufficient controls in place.
The following answers are incorrect:
IS security specialists. Is incorrect because it is not the best answer. Senior management bears the primary responsibility for determining the level of protection needed. Senior security analysts. Is incorrect because it is not the best answer. Senior management bears the primary responsibility for determining the level of protection needed. systems auditors. Is incorrect because it is not the best answer, system auditors are responsible that the controls in place are effective. Senior management bears the primary responsibility for determining the level of protection needed.

QUESTION 264
The security of a computer application is most effective and economical in which of the following cases?

A. The system is optimized prior to the addition of security.
B. The system is procured off-the-shelf.
C. The system is customized to meet the specific security threat.
D. The system is originally designed to provide the necessary security.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The earlier in the process that security is planned for and implement the cheaper it is. It is also much more efficient if security is addressed in each phase of the development cycle rather than an add-on because it gets more complicated to add at the end. If security plan is developed at the beginning it ensures that security won't be overlooked.
The following answers are incorrect:
The system is optimized prior to the addition of security. Is incorrect because if you wait to implement security

after a system is completed the cost of adding security increases dramtically and can become much more complex.
The system is procured off-the-shelf. Is incorrect because it is often difficult to add security to offthe shelf systems.
The system is customized to meet the specific security threat. Is incorrect because this is a distractor. This implies only a single threat.

QUESTION 265
If an operating system permits shared resources such as memory to be used sequentially by multiple users/ application or subjects without a refresh of the objects/memory area, what security problem is MOST likely to exist?

A. Disclosure of residual data.
B. Unauthorized obtaining of a privileged execution state.
C. Data leakage through covert channels.
D. Denial of service through a deadly embrace.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Allowing objects to be used sequentially by multiple users without a refresh of the objects can lead to disclosure of residual data. It is important that steps be taken to eliminate the chance for the disclosure of residual data.
Object reuse refers to the allocation or reallocation of system resources to a user or, more appropriately, to an application or process. Applications and services on a computer system may create or use objects in memory and in storage to perform programmatic functions. In some cases, it is necessary to share these resources between various system applications. However, some objects may be employed by an application to perform privileged tasks on behalf of an authorized user or upstream application. If object usage is not controlled or the data in those objects is not erased after use, they may become available to unauthorized users or processes.
Disclosure of residual data and Unauthorized obtaining of a privileged execution state are both a problem with shared memory and resources. Not clearing the heap/stack can result in residual data and may also allow the user to step on somebody's session if the security token/identify was maintained in that space. This is generally more malicious and intentional than accidental though. The MOST common issue would be Disclosure of residual data.
The following answers are incorrect:
Unauthorized obtaining of a privileged execution state. Is incorrect because this is not a problem with Object Reuse.
Data leakage through covert channels. Is incorrect because it is not the best answer. A covert channel is a communication path. Data leakage would not be a problem created by Object Reuse. In computer security, a covert channel is a type of computer security attack that creates a capability to transfer information objects between processes that are not supposed to be allowed to communicate by the computer security policy. The term, originated in 1973 by Lampson is defined as "(channels) not intended for information transfer at all, such as the service program's effect on system load." to distinguish it from Legitimate channels that are subjected to access controls by COMPUSEC.
Denial of service through a deadly embrace. Is incorrect because it is only a detractor.

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 4174-4179). Auerbach Publications. Kindle Edition.
and
https://www.fas.org/irp/nsa/rainbow/tg018.htm
and
http://en.wikipedia.org/wiki/Covert_channel

QUESTION 266
The Information Technology Security Evaluation Criteria (ITSEC) was written to address which of the following that the Orange Book did not address?

A. integrity and confidentiality.
B. confidentiality and availability.
C. integrity and availability.
D. none of the above.

Correct Answer: C
Explanation

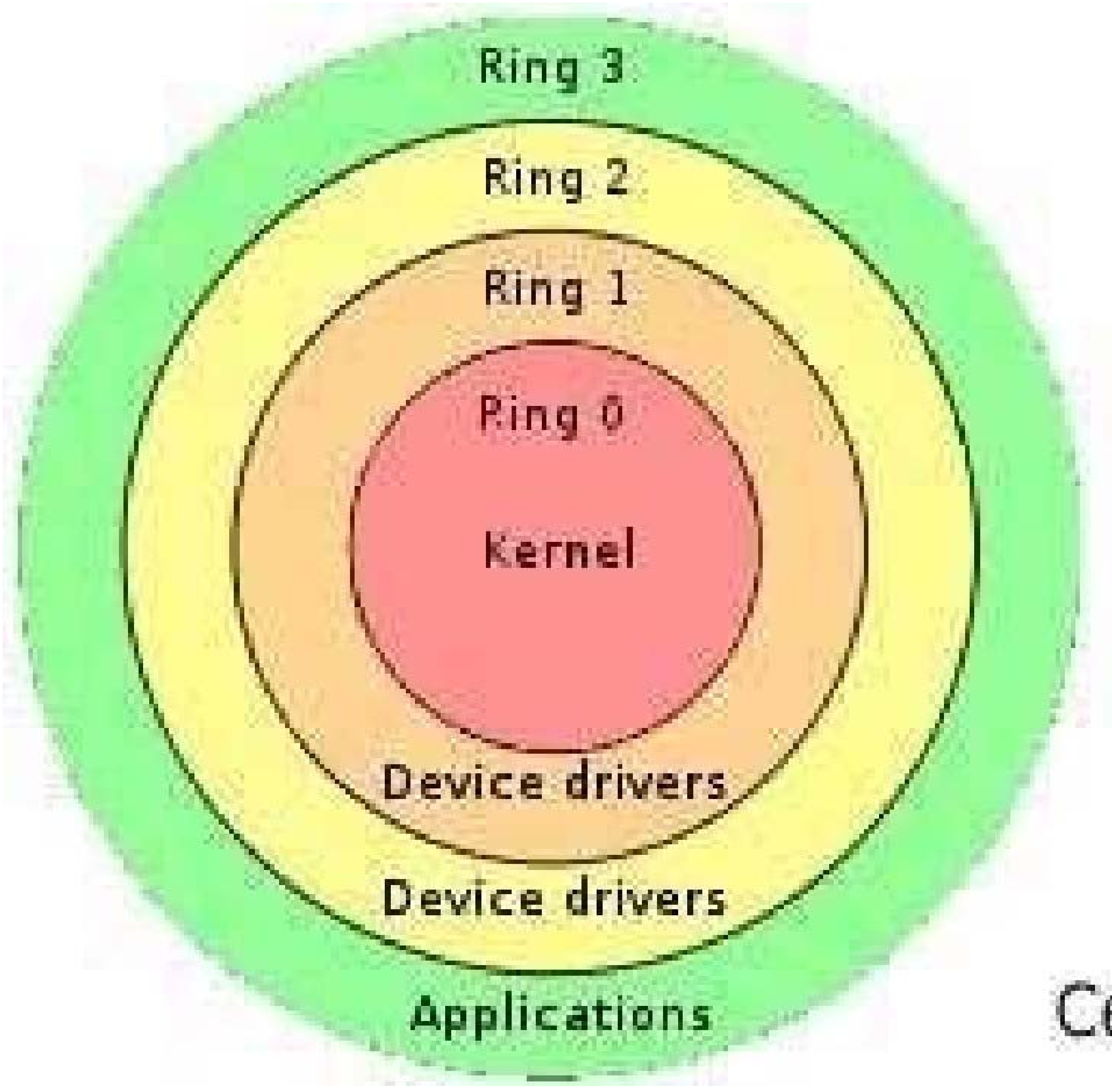
Explanation/Reference:
Explanation: TCSEC focused on confidentiality while ITSEC added integrity and availability as security goals.
The following answers are incorrect:
integrity and confidentiality. Is incorrect because TCSEC addressed confidentiality. confidentiality and availability. Is incorrect because TCSEC addressed confidentiality. none of the above. Is incorrect because ITSEC added integrity and availability as security goals.

QUESTION 267
An Architecture where there are more than two execution domains or privilege levels is called:

A. Ring Architecture.
B. Ring Layering
C. Network Environment.
D. Security Models

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: In computer science, hierarchical protection domains, often called protection rings, are a mechanism to protect data and functionality from faults (fault tolerance) and malicious behavior (computer security). This approach is diametrically opposite to that of capability-based security.
Computer operating systems provide different levels of access to resources. A protection ring is one of two or more hierarchical levels or layers of privilege within the architecture of a computer system. This is generally hardware-enforced by some CPU architectures that provide different CPU modes at the hardware or microcode level. Rings are arranged in a hierarchy from most privileged (most trusted, usually numbered zero) to least privileged (least trusted, usually with the highest ring number). On most operating systems, Ring 0 is the level with the most privileges and interacts most directly with the physical hardware such as the CPU and memory. Special gates between rings are provided to allow an outer ring to access an inner ring's resources in a predefined manner, as opposed to allowing arbitrary usage. Correctly gating access between rings can improve security by preventing programs from one ring or privilege level from misusing resources intended for programs in another. For example, spyware running as a user program in Ring 3 should be prevented from turning on a web camera without informing the user, since hardware access should be a Ring 1 function reserved for device drivers. Programs such as web browsers running in higher numbered rings must request access to the network, a resource restricted to a lower numbered ring.
Ring Architecture



All of the other answers are incorrect because they are detractors.

OIG CBK Security Architecture and Models (page 311)
and
https://en.wikipedia.org/wiki/Ring_%28computer_security%29

QUESTION 268
Which of the following is commonly used for retrofitting multilevel security to a database management system?

A. trusted front-end.

B. trusted back-end.

C. controller.

D. kernel.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: If you are "retrofitting" that means you are adding to an existing database management system (DBMS). You could go back and redesign the entire DBMS but the cost of that could be expensive and there is no telling what the effect will be on existing applications, but that is redesigning and the question states retrofitting. The most cost effective way with the least effect on existing applications while adding a layer of security on top is through a trusted front-end. Clark-Wilson is a synonym of that model as well. It was used to add more granular control or control to database that did not provide appropriate controls or no controls at all. It is one of the most popular model today. Any dynamic website with a back-end database is an example of this today.
Such a model would also introduce separation of duties by allowing the subject only specific rights on the objects they need to access.
The following answers are incorrect:
trusted back-end. Is incorrect because a trusted back-end would be the database management system (DBMS). Since the question stated "retrofitting" that eliminates this answer. controller. Is incorrect because this is a distractor and has nothing to do with "retrofitting". kernel. Is incorrect because this is a distractor and has nothing to do with "retrofitting". A security kernel would provide protection to devices and processes but would be inefficient in protecting rows or columns in a table.

QUESTION 269
Who can best decide what are the adequate technical security controls in a computer-based application system in regards to the protection of the data being used, the criticality of the data, and it's sensitivity level ?

A. System Auditor

B. Data or Information Owner

C. System Manager

D. Data or Information user

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The data or information owner also referred to as "Data Owner" would be the best person. That is the individual or officer who is ultimately responsible for the protection of the information and can therefore decide what are the adequate security controls according to the data sensitivity and data criticality. The auditor would be the best person to determine the adequacy of controls and whether or not they are working as expected by the owner. The function of the auditor is to come around periodically and make sure you are doing what you are supposed to be doing. They ensure the correct controls are in place and are being maintained securely. The goal of the auditor is to make sure the organization complies with its own policies and the applicable laws and regulations.
Organizations can have internal auditors and/ or external auditors. The external auditors commonly work on behalf of a regulatory body to make sure compliance is being met. For example CobiT, which is a model that most information security auditors follow when evaluating a security program. While many security professionals fear and dread auditors, they can be valuable tools in ensuring the overall security of the organization. Their goal is to find the things you have missed and help you understand how to fix the problem.
The Official ISC2 Guide (OIG) says:
IT auditors determine whether users, owners, custodians, systems, and networks are in compliance with the security policies, procedures, standards, baselines, designs, architectures, management direction, and other requirements placed on systems. The auditors provide independent assurance to the management on the appropriateness of the security controls. The auditor examines the information systems and determines whether they are designed, configured, implemented, operated, and managed in a way ensuring that the

organizational objectives are being achieved. The auditors provide top company management with an independent view of the controls and their effectiveness.
Bob is the head of payroll. He is therefore the individual with primary responsibility over the payroll database, and is therefore the information/data owner of the payroll database. In Bob's department, he has Sally and Richard working for him. Sally is responsible for making changes to the payroll database, for example if someone is hired or gets a raise. Richard is only responsible for printing paychecks. Given those roles, Sally requires both read and write access to the payroll database, but Richard requires only read access to it. Bob communicates these requirements to the system administrators (the "information/data custodians") and they set the file permissions for Sally's and Richard's user accounts so that Sally has read/write access, while Richard has only read access.
So in short Bob will determine what controls are required, what is the sensitivily and criticality of the Data. Bob will communicate this to the custodians who will implement the requirements on the systems/DB. The auditor would assess if the controls are in fact providing the level of security the Data Owner expects within the systems/DB. The auditor does not determine the sensitivity of the data or the crititicality of the data.
The other answers are not correct because:
A "system auditor" is never responsible for anything but auditing... not actually making control decisions but the auditor would be the best person to determine the adequacy of controls and then make recommendations.
A "system manager" is really just another name for a system administrator, which is actually an information custodian as explained above.
A "Data or information user" is responsible for implementing security controls on a day-to-day basis as they utilize the information, but not for determining what the controls should be or if they are adequate.

Official ISC2 Guide to the CISSP CBK, Third Edition , Page 477 Schneiter, Andrew (2013-04-15). Official (ISC) 2 Guide to the CISSP CBK, Third Edition :
Information Security Governance and Risk Management ((ISC)2 Press) (Kindle Locations 294- 298). Auerbach Publications. Kindle Edition.
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 3108- 3114).
Information Security Glossary
Responsibility for use of information resources

QUESTION 270
A security evaluation report and an accreditation statement are produced in which of the following phases of the system development life cycle?

A. project initiation and planning phase
B. system design specification phase
C. development & documentation phase
D. acceptance phase

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The
Answer: "acceptance phase". Note the question asks about an "evaluation report" - which details how the system evaluated, and an "accreditation statement" which describes the level the system is allowed to operate at. Because those two activities are a part of testing and testing is a part of the acceptance phase, the only answer above that can be correct is "acceptance phase".
The other answers are not correct because:
The "project initiation and planning phase" is just the idea phase. Nothing has been developed yet to be evaluated, tested, accredited, etc.
The "system design specification phase" is essentially where the initiation and planning phase is fleshed out. For example, in the initiation and planning phase, we might decide we want the system to have authentication. In the design specification phase, we decide that that authentication will be accomplished via username/ password. But there is still nothing actually developed at this point to evaluate or accredit.
The "development & documentation phase" is where the system is created and documented. Part of the documentation includes specific evaluation and accreditation criteria. That is the criteria that will be used to evaluate and accredit the system during the "acceptance phase". In other words - you cannot evaluate or

accredit a system that has not been created yet. Of the four answers listed, only the acceptance phase is dealing with an existing system. The others deal with planning and creating the system, but the actual system isn't there yet.
Official ISC2 Guide Page: 558 - 559
All in One Third Edition page: 832 - 833 (recommended reading)

QUESTION 271
Which of the following is often the greatest challenge of distributed computing solutions?

A. scalability
B. security
C. heterogeneity
D. usability

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The correct answer to this "security". It is a major factor in deciding if a centralized or decentralized environment is more appropriate.
Example: In a centralized computing environment, you have a central server and workstations (often "dumb terminals") access applications, data, and everything else from that central servers. Therefore, the vast majority of your security resides on a centrally managed server. In a decentralized (or distributed) environment, you have a collection of PC's each with their own operating systems to maintain, their own software to maintain, local data storage requiring protection and backup. You may also have PDA's and "smart phones", data watches, USB devices of all types able to store data... the list gets longer all the time. It is entirely possible to reach a reasonable and acceptable level of security in a distributed environment. But doing so is significantly more difficult, requiring more effort, more money, and more time.
The other answers are not correct because:
scalability - A distributed computing environment is almost infinitely scalable. Much more so than a centralized environment. This is therefore a bad answer. heterogeneity - Having products and systems from multiple vendors in a distributed environment is significantly easier than in a centralized environment. This would not be a "challenge of distributed computing solutions" and so is not a good answer.
usability - This is potentially a challenge in either environment, but whether or not this is a problem has very little to do with whether it is a centralized or distributed environment. Therefore, this would not be a good answer.
Official ISC2 Guide page: 313-314
All in One Third Edition page: (unavailable at this time)

QUESTION 272
What is the appropriate role of the security analyst in the application system development or acquisition project?

A. policeman
B. control evaluator & consultant
C. data owner
D. application user

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The correct answer is "control evaluator & consultant". During any system development or acquisition, the security staff should evaluate security controls and advise (or consult) on the strengths and weaknesses with those responsible for making the final decisions on the project.
The other answers are not correct because:
policeman - It is never a good idea for the security staff to be placed into this type of role (though it is

sometimes unavoidable). During system development or acquisition, there should be no need of anyone filling the role of policeman.
data owner - In this case, the data owner would be the person asking for the new system to manage, control, and secure information they are responsible for. While it is possible the security staff could also be the data owner for such a project if they happen to have responsibility for the information, it is also possible someone else would fill this role. Therefore, the best answer remains "control evaluator & consultant".
application user - Again, it is possible this could be the security staff, but it could also be many other people or groups. So this is not the best answer.
Official ISC2 Guide page: 555 - 560
All in One Third Edition page: 832 - 846

QUESTION 273
The information security staff's participation in which of the following system development life cycle phases provides maximum benefit to the organization?

A. project initiation and planning phase
B. system design specifications phase
C. development and documentation phase
D. in parallel with every phase throughout the project

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The other answers are not correct because:
You are always looking for the "best" answer. While each of the answers listed here could be considered correct in that each of them require input from the security staff, the best answer is for that input to happen at all phases of the project.
Official ISC2 Guide page: 556
All in One Third Edition page: 832 - 833

QUESTION 274
Which of the following is NOT an example of an operational control?

A. backup and recovery
B. Auditing
C. contingency planning
D. operations procedures

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Operational controls are controls over the hardware, the media used and the operators using these resources.
Operational controls are controls that are implemented and executed by people, they are most often procedures.
Backup and recovery, contingency planning and operations procedures are operational controls. Auditing is considered an Administrative / detective control. However the actual auditing mechanisms in place on the systems would be consider operational controls.

QUESTION 275
Degaussing is used to clear data from all of the following medias except:

A. Floppy Disks
B. Read-Only Media

C. Video Tapes

D. Magnetic Hard Disks

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Atoms and Data
Shon Harris says: "A device that performs degaussing generates a coercive magnetic force that reduces the magnetic flux density of the storage media to zero. This magnetic force is what properly erases data from media. Data are stored on magnetic media by the representation of the polarization of the atoms. Degaussing changes"
The latest ISC2 book says:
"Degaussing can also be a form of media destruction. High-power degaussers are so strong in some cases that they can literally bend and warp the platters in a hard drive. Shredding and burning are effective destruction methods for non-rigid magnetic media. Indeed, some shredders are capable of shredding some rigid media such as an optical disk. This may be an effective alternative for any optical media containing nonsensitive information due to the residue size remaining after feeding the disk into the machine. However, the residue size might be too large for media containing sensitive information. Alternatively, grinding and pulverizing are acceptable choices for rigid and solid-state media. Specialized devices are available for grinding the face of optical media that either sufficiently scratches the surface to render the media unreadable or actually grinds off the data layer of the disk. Several services also exist which will collect drives, destroy them on site if requested and provide certification of completion. It will be the responsibility of the security professional to help, select, and maintain the most appropriate solutions for media cleansing and disposal."
Degaussing is achieved by passing the magnetic media through a powerful magnet field to rearrange the metallic particles, completely removing any resemblance of the previously recorded signal (from the "all about degaussers link below). Therefore, degaussing will work on any electronic based media such as floppy disks, or hard disks - all of these are examples of electronic storage. However, "read-only media" includes items such as paper printouts and CD-ROM wich do not store data in an electronic form or is not magnetic storage. Passing them through a magnet field has no effect on them.
Not all clearing/ purging methods are applicable to all media-- for example, optical media is not susceptible to degaussing, and overwriting may not be effective against Flash devices. The degree to which information may be recoverable by a sufficiently motivated and capable adversary must not be underestimated or guessed at in ignorance. For the highest-value commercial data, and for all data regulated by government or military classification rules, read and follow the rules and standards.
I will admit that this is a bit of a trick question. Determining the difference between "read-only media" and "read-only memory" is difficult for the question taker. However, I believe it is representative of the type of question you might one day see on an exam.
The other answers are incorrect because:
Floppy Disks, Magnetic Tapes, and Magnetic Hard Disks are all examples of magnetic storage, and therefore are erased by degaussing.
A videotape is a recording of images and sounds on to magnetic tape as opposed to film stock used in filmmaking or random access digital media. Videotapes are also used for storing scientific or medical data, such as the data produced by an electrocardiogram. In most cases, a helical scan video head rotates against the moving tape to record the data in two dimensions, because video signals have a very high bandwidth, and static heads would require extremely high tape speeds. Videotape is used in both video tape recorders (VTRs) or, more commonly and more recently, videocassette recorder (VCR) and camcorders. A Tape use a linear method of storing information and since nearly all video recordings made nowadays are digital direct to disk recording (DDR), videotape is expected to gradually lose importance as non-linear/random-access methods of storing digital video data become more common.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 25627- 25630). McGraw-Hill. Kindle Edition.
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Security Operations (Kindle Locations 580-588). . Kindle Edition.
All About Degaussers and Erasure of Magnetic Media:
http://www.degausser.co.uk/degauss/degabout.htm
http://www.degaussing.net/
http://www.cerberussystems.com/INFOSEC/stds/ncsctg25.htm

QUESTION 276
It is a violation of the "separation of duties" principle when which of the following individuals access the software on systems implementing security?

A. security administrator
B. security analyst
C. systems auditor
D. systems programmer

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The security administrator, security analysis, and the system auditor need access to portions of the security systems to accomplish their jobs. The system programmer does not need access to the working (AKA: Production) security systems. Programmers should not be allowed to have ongoing direct access to computers running production systems (systems used by the organization to operate its business). To maintain system integrity, any changes they make to production systems should be tracked by the organization's change management control system.
Because the security administrator's job is to perform security functions, the performance of nonsecurity tasks must be strictly limited. This separation of duties reduces the likelihood of loss that results from users abusing their authority by taking actions outside of their assigned functional responsibilities.

OFFICIAL (ISC)2® GUIDE TO THE CISSP® EXAM (2003), Hansche, S., Berti, J., Hare, H., Auerbach Publication, FL, Chapter 5 - Operations Security, section 5.3,"Security Technology and Tools," Personnel section (page 32).
KRUTZ, R. & VINES, R. The CISSP Prep Guide: Gold Edition (2003), Wiley Publishing Inc., Chapter 6: Operations Security, Separations of Duties (page 303).

QUESTION 277
When backing up an applications system's data, which of the following is a key question to be answered first?

A. When to make backups
B. Where to keep backups
C. What records to backup
D. How to store backups

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: It is critical that a determination be made of WHAT data is important and should be retained and protected. Without determining the data to be backed up, the potential for error increases. A record or file could be vital and yet not included in a backup routine. Alternatively, temporary or insignificant files could be included in a backup routine unnecessarily.
The following answers were incorrect:
When to make backups Although it is important to consider schedules for backups, this is done after the decisions are made of what should be included in the backup routine. Where to keep backups The location of storing backup copies of data (Such as tapes, on-line backups, etc) should be made after determining what should be included in the backup routine and the method to store the backup.
How to store backups The backup methodology should be considered after determining what data should be included in the backup routine.

QUESTION 278
A 'Pseudo flaw' is which of the following?

A. An apparent loophole deliberately implanted in an operating system program as a trap for intruders.
B. An omission when generating Psuedo-code.
C. Used for testing for bounds violations in application programming.
D. A normally generated page fault causing the system to halt.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: A Pseudo flaw is something that looks like it is vulnerable to attack, but really acts as an alarm or triggers automatic actions when an intruder attempts to exploit the flaw.
The following answers are incorrect:
An omission when generating Psuedo-code. Is incorrect because it is a distractor. Used for testing for bounds violations in application programming. Is incorrect, this is a testing methodology.
A normally generated page fault causing the system to halt. This is incorrect because it is distractor.

QUESTION 279
Which of the following is considered the weakest link in a security system?

A. People
B. Software
C. Communications
D. Hardware

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The
Answer: People. The other choices can be strengthened and counted on (For the most part) to remain consistent if properly protected. People are fallible and unpredictable. Most security intrusions are caused by employees. People get tired, careless, and greedy. They are not always reliable and may falter in following defined guidelines and best practices. Security professionals must install adequate prevention and detection controls and properly train all systems users Proper hiring and firing practices can eliminate certain risks. Security Awareness training is key to ensuring people are aware of risks and their responsibilities. The following answers are incorrect:Software. Although software exploits are major threat and cause for concern, people are the weakest point in a security posture. Software can be removed, upgraded or patched to reduce risk.
Communications. Although many attacks from inside and outside an organization use communication methods such as the network infrastructure, this is not the weakest point in a security posture. Communications can be monitored, devices installed or upgraded to reduce risk and react to attack attempts.
Hardware. Hardware components can be a weakness in a security posture, but they are not the weakest link of the choices provided. Access to hardware can be minimized by such measures as installing locks and monitoring access in and out of certain areas. The following reference(s) were/was used to create this question:
Shon Harris AIO v.3 P.19, 107-109
ISC2 OIG 2007, p.51-55

QUESTION 280
Which of the following is based on the premise that the quality of a software product is a direct function of the quality of its associated software development and maintenance processes?

A. The Software Capability Maturity Model (CMM)
B. The Spiral Model
C. The Waterfall Model
D. Expert Systems Model

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The Capability Maturity Model (CMM) is a service mark owned by Carnegie Mellon University (CMU) and refers to a development model elicited from actual data. The data was collected from organizations that contracted with the U.S. Department of Defense, who funded the research, and became the foundation from which CMU created the Software Engineering Institute (SEI). Like any model, it is an abstraction of an existing system. The Capability Maturity Model (CMM) is a methodology used to develop and refine an organization's software development process. The model describes a five-level evolutionary path of increasingly organized and systematically more mature processes. CMM was developed and is promoted by the Software Engineering Institute (SEI), a research and development center sponsored by the U.S. Department of Defense (DoD). SEI was founded in 1984 to address software engineering issues and, in a broad sense, to advance software engineering methodologies. More specifically, SEI was established to optimize the process of developing, acquiring, and maintaining heavily software-reliant systems for the DoD. Because the processes involved are equally applicable to the software industry as a whole, SEI advocates industry-wide adoption of the CMM.

The CMM is similar to ISO 9001, one of the ISO 9000 series of standards specified by the International Organization for Standardization (ISO). The ISO 9000 standards specify an effective quality system for manufacturing and service industries; ISO 9001 deals specifically with software development and maintenance. The main difference between the two systems lies in their respective purposes: ISO 9001 specifies a minimal acceptable quality level for software processes, while the CMM establishes a framework for continuous process improvement and is more explicit than the ISO standard in defining the means to be employed to that end.

CMM's Five Maturity Levels of Software Processes

At the initial level, processes are disorganized, even chaotic. Success is likely to depend on individual efforts, and is not considered to be repeatable, because processes would not be sufficiently defined and documented to allow them to be replicated. At the repeatable level, basic project management techniques are established, and successes could be repeated, because the requisite processes would have been made established, defined, and documented.

At the defined level, an organization has developed its own standard software process through greater attention to documentation, standardization, and integration. At the managed level, an organization monitors and controls its own processes through data collection and analysis.

At the optimizing level, processes are constantly being improved through monitoring feedback from current processes and introducing innovative processes to better serve the organization's particular needs.

When it is applied to an existing organization's software development processes, it allows an effective approach toward improving them. Eventually it became clear that the model could be applied to other processes. This gave rise to a more general concept that is applied to business processes and to developing people.

CMM is superseded by CMMI

The CMM model proved useful to many organizations, but its application in software development has sometimes been problematic. Applying multiple models that are not integrated within and across an organization could be costly in terms of training, appraisals, and improvement activities. The Capability Maturity Model Integration (CMMI) project was formed to sort out the problem of using multiple CMMs.

For software development processes, the CMM has been superseded by Capability Maturity Model Integration (CMMI), though the CMM continues to be a general theoretical process capability model used in the public domain.

CMM is adapted to processes other than software development The CMM was originally intended as a tool to evaluate the ability of government contractors to perform a contracted software project. Though it comes from the area of software development, it can be, has been, and continues to be widely applied as a general model of the maturity of processes (e.g., IT Service Management processes) in IS/IT (and other) organizations.

Source:
http://searchsoftwarequality.techtarget.com/sDefinition/0,,sid92_gci930057,00.html and
http://en.wikipedia.org/wiki/Capability_Maturity_Model

QUESTION 281
Which of the following determines that the product developed meets the projects goals?

A. verification
B. validation
C. concurrence
D. accuracy

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Software Development Verification vs. Validation:
Verification determines if the product accurately represents and meets the design specifications given to the developers. A product can be developed that does not match the original specifications. This step ensures that the specifications are properly met and closely followed by the development team.
Validation determines if the product provides the necessary solution intended real-world problem. It validates whether or not the final product is what the user expected in the first place and whether or not it solve the problem it intended to solve. In large projects, it is easy to lose sight of overall goal. This exercise ensures that the main goal of the project is met.
From DITSCAP:
6.3.2. Phase 2, Verification. The Verification phase shall include activities to verify compliance of the system with previously agreed security requirements. For each life-cycle development activity, DoD Directive 5000.1 (reference (i)), there is a corresponding set of security activities, enclosure 3, that shall verify compliance with the security requirements and evaluate vulnerabilities. 6.3.3. Phase 3, Validation. The Validation phase shall include activities to evaluate the fully integrated system to validate system operation in a specified computing environment with an acceptable level of residual risk. Validation shall culminate in an approval to operate.
NOTE:
DIACAP has replace DITSCAP but the definition above are still valid and applicable for the purpose of the exam.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 1106). McGraw-Hill.
Kindle Edition.
and
http://iase.disa.mil/ditscap/DITSCAP.html

QUESTION 282
Which of the following is the act of performing tests and evaluations to test a system's security level to see if it complies with the design specifications and security requirements?

A. Validation
B. Verification
C. Assessment
D. Accuracy

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Verification vs. Validation:
Verification determines if the product accurately represents and meets the specifications. A product can be developed that does not match the original specifications. This step ensures that the specifications are properly met.
Validation determines if the product provides the necessary solution intended real-world problem. In large projects, it is easy to lose sight of overall goal. This exercise ensures that the main goal of the project is met.
From DITSCAP:
6.3.2. Phase 2, Verification. The Verification phase shall include activities to verify compliance of the system with previously agreed security requirements. For each life-cycle development activity, DoD Directive 5000.1 (reference (i)), there is a corresponding set of security activities, enclosure 3, that shall verify compliance with the security requirements and evaluate vulnerabilities. 6.3.3. Phase 3, Validation. The Validation phase shall

include activities to evaluate the fully integrated system to validate system operation in a specified computing environment with an acceptable level of residual risk. Validation shall culminate in an approval to operate. You must also be familiar with Verification and Validation for the purpose of the exam. A simple definition for Verification would be whether or not the developers followed the design specifications along with the security requirements. A simple definition for Validation would be whether or not the final product meets the end user needs and can be use for a specific purpose. Wikipedia has an informal description that is currently written as: Validation can be expressed by the query "Are you building the right thing?" and Verification by "Are you building it right? NOTE:
DITSCAP was replaced by DIACAP some time ago (2007). While DITSCAP had defined both a verification and a validation phase, the DIACAP only has a validation phase. It may not make a difference in the answer for the exam; however, DIACAP is the cornerstone policy of DOD C&A and IA efforts today. Be familiar with both terms just in case all of a sudden the exam becomes updated with the new term.
Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 1106). McGraw-Hill.
Kindle Edition.
http://iase.disa.mil/ditscap/DITSCAP.html
https://en.wikipedia.org/wiki/Verification_and_validation For the definition of "validation" in DIACAP, Click Here Further sources for the phases in DIACAP, Click Here

QUESTION 283
Which of the following refers to the data left on the media after the media has been erased?

A. remanence
B. recovery
C. sticky bits
D. semi-hidden

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Actually the term "remanence" comes from electromagnetism, the study of the electromagnetics. Originally referred to (and still does in that field of study) the magnetic flux that remains in a magnetic circuit after an applied magnetomotive force has been removed. Absolutely no way a candidate will see anywhere near that much detail on any similar CISSP question, but having read this, a candidate won't be likely to forget it either. It is becoming increasingly commonplace for people to buy used computer equipment, such as a hard drive, or router, and find information on the device left there by the previous owner; information they thought had been deleted. This is a classic example of data remanence: the remains of partial or even the entire data set of digital information. Normally, this refers to the data that remain on media after they are written over or degaussed. Data remanence is most common in storage systems but can also occur in memory.
Specialized hardware devices known as degaussers can be used to erase data saved to magnetic media. The measure of the amount of energy needed to reduce the magnetic field on the media to zero is known as coercivity.
It is important to make sure that the coercivity of the degausser is of sufficient strength to meet object reuse requirements when erasing data. If a degausser is used with insufficient coercivity, then a remanence of the data will exist. Remanence is the measure of the existing magnetic field on the media; it is the residue that remains after an object is degaussed or written over. Data is still recoverable even when the remanence is small. While data remanence exists, there is no assurance of safe object reuse.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 4207-4210). Auerbach Publications. Kindle Edition.
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 19694-19699). Auerbach Publications. Kindle Edition.

QUESTION 284
Which of the following is NOT a basic component of security architecture?

A. Motherboard

B. Central Processing Unit (CPU

C. Storage Devices

D. Peripherals (input/output devices)

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The CPU, storage devices and peripherals each have specialized roles in the security archecture. The CPU, or microprocessor, is the brains behind a computer system and performs calculations as it solves problemes and performs system tasks. Storage devices provide both long- and short-term stoarge of information that the CPU has either processed or may process. Peripherals (scanners, printers, modems, etc) are devices that either input datra or receive the data output by the CPU.
The motherboard is the main circuit board of a microcomputer and contains the connectors for attaching additional boards. Typically, the motherboard contains the CPU, BIOS, memory, mass storage interfaces, serial and parallel ports, expansion slots, and all the controllers required to control standard peripheral devices.
Reference(s) used for this question:
TIPTON, Harold F., The Official (ISC)2 Guide to the CISSP CBK (2007), page 308.

QUESTION 285
Which of the following is a set of data processing elements that increases the performance in a computer by overlapping the steps of different instructions?

A. pipelining

B. complex-instruction-set-computer (CISC)

C. reduced-instruction-set-computer (RISC)

D. multitasking

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Pipelining is a natural concept in everyday life, e.g. on an assembly line. Consider the assembly of a car: assume that certain steps in the assembly line are to install the engine, install the hood, and install the wheels (in that order, with arbitrary interstitial steps). A car on the assembly line can have only one of the three steps done at once. After the car has its engine installed, it moves on to having its hood installed, leaving the engine installation facilities available for the next car. The first car then moves on to wheel installation, the second car to hood installation, and a third car begins to have its engine installed. If engine installation takes 20 minutes, hood installation takes 5 minutes, and wheel installation takes 10 minutes, then finishing all three cars when only one car can be assembled at once would take 105 minutes. On the other hand, using the assembly line, the total time to complete all three is 75 minutes. At this point, additional cars will come off the assembly line at 20 minute increments. In computing, a pipeline is a set of data processing elements connected in series, so that the output of one element is the input of the next one. The elements of a pipeline are often executed in parallel or in time-sliced fashion; in that case, some amount of buffer storage is often inserted between elements. Pipelining is used in processors to allow overlapping execution of multiple instructions within the same circuitry. The circuitry is usually divided into stages, including instruction decoding, arithmetic, and register fetching stages, wherein each stage processes one instruction at a time.
The following were not correct answers:
CISC: is a CPU design where single instructions execute several low-level operations (such as a load from memory, an arithmetic operation, and a memory store) within a single instruction. RISC: is a CPU design based on simplified instructions that can provide higher performance as the simplicity enables much faster execution of each instruction. Multitasking: is a method where multiple tasks share common processing resources, such as a CPU, through a method of fast scheduling that gives the appearance of parallelism, but in reality only one task is being performed at any one time.
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer

Security, pages 188-189.
Also see
http://en.wikipedia.org/wiki/Pipeline_(computing)

QUESTION 286
Which of the following describes a computer processing architecture in which a language compiler or pre-processor breaks program instructions down into basic operations that can be performed by the processor at the same time?

A. Very-Long Instruction-Word Processor (VLIW)
B. Complex-Instruction-Set-Computer (CISC)
C. Reduced-Instruction-Set-Computer (RISC)
D. Super Scalar Processor Architecture (SCPA)

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Very long instruction word (VLIW) describes a computer processing architecture in which a language compiler or pre-processor breaks program instruction down into basic operations that can be performed by the processor in parallel (that is, at the same time). These operations are put into a very long instruction word which the processor can then take apart without further analysis, handing each operation to an appropriate functional unit.
The following answer are incorrect:
The term "CISC" (complex instruction set computer or computing) refers to computers designed with a full set of computer instructions that were intended to provide needed capabilities in the most efficient way. Later, it was discovered that, by reducing the full set to only the most frequently used instructions, the computer would get more work done in a shorter amount of time for most applications. Intel's Pentium microprocessors are CISC microprocessors. The PowerPC microprocessor, used in IBM's RISC System/6000 workstation and Macintosh computers, is a RISC microprocessor. RISC takes each of the longer, more complex instructions from a CISC design and reduces it to multiple instructions that are shorter and faster to process. RISC technology has been a staple of mobile devices for decades, but it is now finally poised to take on a serious role in data center servers and server virtualization. The latest RISC processors support virtualization and will change the way computing resources scale to meet workload demands.
A superscalar CPU architecture implements a form of parallelism called instruction level parallelism within a single processor. It therefore allows faster CPU throughput than would otherwise be possible at a given clock rate. A superscalar processor executes more than one instruction during a clock cycle by simultaneously dispatching multiple instructions to redundant functional units on the processor. Each functional unit is not a separate CPU core but an execution resource within a single CPU such as an arithmetic logic unit, a bit shifter, or a multiplier.
Reference(s) Used for this question:
http://whatis.techtarget.com/definition/0,,sid9_gci214395,00.html and
http://searchcio-midmarket.techtarget.com/definition/CISC and
http://en.wikipedia.org/wiki/Superscalar

QUESTION 287
Which of the following addresses a portion of the primary memory by specifying the actual address of the memory location?

A. direct addressing
B. Indirect addressing
C. implied addressing
D. indexed addressing

Correct Answer: A
Explanation

Explanation/Reference:

Explanation: Absolute/Direct

```
+------+-----+--------------------------------------+
| load | reg | address |
+------+-----+--------------------------------------+
```

(Effective address = address as given in instruction)

This requires space in an instruction for quite a large address. It is often available on CISC machines which have variable-length instructions, such as x86. Some RISC machines have a special Load Upper Literal instruction which places a 16-bit constant in the top half of a register. An OR literal instruction can be used to insert a 16-bit constant in the lower half of that register, so that a full 32-bit address can then be used via the register-indirect addressing mode, which itself is provided as "base-plus-offset" with an offset of 0. http://en.wikipedia.org/wiki/Addressing_mode (Very good coverage of the subject) also see:

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, page 186.

also see:

http://www.comsci.us/ic/notes/am.html

QUESTION 288

Which of the following is NOT true concerning Application Control?

A. It limits end users use of applications in such a way that only particular screens are visible.

B. Only specific records can be requested through the application controls

C. Particular usage of the application can be recorded for audit purposes

D. It is non-transparent to the endpoint applications so changes are needed to the applications and databases involved

Correct Answer: D

Explanation

Explanation/Reference:

Explanation: Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, Auerbach.

QUESTION 289

Which of the following are NOT a countermeasure to traffic analysis?

A. Padding messages.

B. Eavesdropping.

C. Sending noise.

D. Faraday Cage

Correct Answer: B

Explanation

Explanation/Reference:

Explanation: Eavesdropping is not a countermeasure, it is a type of attack where you are collecting traffic and attempting to see what is being send between entities communicating with each other.

The following answers are incorrect:

Padding Messages. Is incorrect because it is considered a countermeasure you make messages uniform size, padding can be used to counter this kind of attack, in which decoy traffic is sent out over the network to disguise patterns and make it more difficult to uncover patterns. Sending Noise. Is incorrect because it is considered a countermeasure, tansmitting noninformational data elements to disguise real data.

Faraday Cage Is incorrect because it is a tool used to prevent emanation of electromagnetic waves. It is a very effective tool to prevent traffic analysis.

QUESTION 290

Preservation of confidentiality within information systems requires that the information is not disclosed to:

A. Authorized person
B. Unauthorized persons or processes.
C. Unauthorized persons.
D. Authorized persons and processes

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Confidentiality assures that the information is not disclosed to unauthorized persons or processes.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 31.

QUESTION 291
Which of the following is not one of the three goals of Integrity addressed by the Clark-Wilson model?

A. Prevention of the modification of information by unauthorized users.
B. Prevention of the unauthorized or unintentional modification of information by authorized users.
C. Preservation of the internal and external consistency.
D. Prevention of the modification of information by authorized users.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: There is no need to prevent modification from authorized users. They are authorized and allowed to make the changes. On top of this, it is also NOT one of the goal of Integrity within Clark-Wilson.
As it turns out, the Biba model addresses only the first of the three integrity goals which is Prevention of the modification of information by unauthorized users. Clark-Wilson addresses all three goals of integrity.
The ClarkWilson model improves on Biba by focusing on integrity at the transaction level and addressing three major goals of integrity in a commercial environment. In addition to preventing changes by unauthorized subjects, Clark and Wilson realized that high-integrity systems would also have to prevent undesirable changes by authorized subjects and to ensure that the system continued to behave consistently. It also recognized that it would need to ensure that there is constant mediation between every subject and every object if such integrity was going to be maintained.
Integrity is addressed through the following three goals:
1. Prevention of the modification of information by unauthorized users.
2. Prevention of the unauthorized or unintentional modification of information by authorized users.
3. Preservation of the internal and external consistency. The following reference(s) were used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 17689-17694). Auerbach Publications. Kindle Edition.
and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 31.

QUESTION 292
External consistency ensures that the data stored in the database is:

A. in-consistent with the real world.
B. remains consistant when sent from one system to another.
C. consistent with the logical world.
D. consistent with the real world.

Correct Answer: D

Explanation

Explanation/Reference:
Explanation: External consistency ensures that the data stored in the database is consistent with the real world.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, page 33.

QUESTION 293
Which of the following would be best suited to oversee the development of an information security policy?

A. System Administrators
B. End User
C. Security Officers
D. Security administrators

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The security officer would be the best person to oversea the development of such policies.
Security officers and their teams have typically been charged with the responsibility of creating the security policies. The policies must be written and communicated appropriately to ensure that they can be understood by the end users. Policies that are poorly written, or written at too high of an education level (common industry practice is to focus the content for general users at the sixth- to eighth-grade reading level), will not be understood.
Implementing security policies and the items that support them shows due care by the company and its management staff. Informing employees of what is expected of them and the consequences of noncompliance can come down to a liability issue. While security officers may be responsible for the development of the security policies, the effort should be collaborative to ensure that the business issues are addressed. The security officers will get better corporate support by including other areas in policy development. This helps build buy-in by these areas as they take on a greater ownership of the final product. Consider including areas such as HR, legal, compliance, various IT areas and specific business area representatives who represent critical business units. When policies are developed solely within the IT department and then distributed without business input, they are likely to miss important business considerations. Once policy documents have been created, the basis for ensuring compliance is established. Depending on the organization, additional documentation may be necessary to support policy. This support may come in the form of additional controls described in standards, baselines, or procedures to help personnel with compliance. An important step after documentation is to make the most current version of the documents readily accessible to those who are expected to follow them. Many organizations place the documents on their intranets or in shared file folders to facilitate their accessibility. Such placement of these documents plus checklists, forms, and sample documents can make awareness more effective.
For your exam you should know the information below:
End User - The end user is responsible for protecting information assets on a daily basis through adherence to the security policies that have been communicated. Executive Management/Senior Management - Executive management maintains the overall responsibility for protection of the information assets. The business operations are dependent upon information being available, accurate, and protected from individuals without a need to know. Security Officer - The security officer directs, coordinates, plans, and organizes information security activities throughout the organization. The security officer works with many different individuals, such as executive management, management of the business units, technical staff, business partners, auditors, and third parties such as vendors. The security officer and his or her team are responsible for the design, implementation, management, and review of the organization's security policies, standards, procedures, baselines, and guidelines. Information Systems Security Professional- Drafting of security policies, standards and supporting guidelines, procedures, and baselines is coordinated through these individuals. Guidance is provided for technical security issues, and emerging threats are considered for the adoption of new policies. Activities such as interpretation of government regulations and industry trends and analysis of vendor solutions to include in the security architecture that advances the security of the organization are performed in this role. Data/Information/Business/System Owners - A business executive or manager is typically responsible for an

information asset. These are the individuals that assign the appropriate classification to information assets. They ensure that the business information is protected with appropriate controls. Periodically, the information asset owners need to review the classification and access rights associated with information assets. The owners, or their delegates, may be required to approve access to the information. Owners also need to determine the criticality, sensitivity, retention, backups, and safeguards for the information. Owners or their delegates are responsible for understanding the risks that exist with regards to the information that they control. Data/Information Custodian/Steward - A data custodian is an individual or function that takes care of the information on behalf of the owner. These individuals ensure that the information is available to the end users and is backed up to enable recovery in the event of data loss or corruption. Information may be stored in files, databases, or systems whose technical infrastructure must be managed, by systems administrators. This group administers access rights to the information assets.

Information Systems Auditor- IT auditors determine whether users, owners, custodians, systems, and networks are in compliance with the security policies, procedures, standards, baselines, designs, architectures, management direction, and other requirements placed on systems. The auditors provide independent assurance to the management on the appropriateness of the security controls. The auditor examines the information systems and determines whether they are designed, configured, implemented, operated, and managed in a way ensuring that the organizational objectives are being achieved. The auditors provide top company management with an independent view of the controls and their effectiveness. Business Continuity Planner - Business continuity planners develop contingency plans to prepare for any occurrence that could have the ability to impact the company's objectives negatively. Threats may include earthquakes, tornadoes, hurricanes, blackouts, changes in the economic/political climate, terrorist activities, fire, or other major actions potentially causing significant harm. The business continuity planner ensures that business processes can continue through the disaster and coordinates those activities with the business areas and information technology personnel responsible for disaster recovery. Information Systems/ Technology Professionals- These personnel are responsible for designing security controls into information systems, testing the controls, and implementing the systems in production environments through agreed upon operating policies and procedures. The information systems professionals work with the business owners and the security professionals to ensure that the designed solution provides security controls commensurate with the acceptable criticality, sensitivity, and availability requirements of the application. Security Administrator - A security administrator manages the user access request process and ensures that privileges are provided to those individuals who have been authorized for access by application/system/data owners. This individual has elevated privileges and creates and deletes accounts and access permissions. The security administrator also terminates access privileges when individuals leave their jobs or transfer between company divisions. The security administrator maintains records of access request approvals and produces reports of access rights for the auditor during testing in an access controls audit to demonstrate compliance with the policies.

Network/Systems Administrator - A systems administrator (sysadmin/netadmin) configures network and server hardware and the operating systems to ensure that the information can be available and accessible. The administrator maintains the computing infrastructure using tools and utilities such as patch management and software distribution mechanisms to install updates and test patches on organization computers. The administrator tests and implements system upgrades to ensure the continued reliability of the servers and network devices. The administrator provides vulnerability management through either commercial off the shelf (COTS) and/or non-COTS solutions to test the computing environment and mitigate vulnerabilities appropriately. Physical Security - The individuals assigned to the physical security role establish relationships with external law enforcement, such as the local police agencies, state police, or the Federal Bureau of Investigation (FBI) to assist in investigations. Physical security personnel manage the installation, maintenance, and ongoing operation of the closed circuit television (CCTV) surveillance systems, burglar alarm systems, and card reader access control systems. Guards are placed where necessary as a deterrent to unauthorized access and to provide safety for the company employees. Physical security personnel interface with systems security, human resources, facilities, and legal and business areas to ensure that the practices are integrated. Security Analyst - The security analyst role works at a higher, more strategic level than the previously described roles and helps develop policies, standards, and guidelines, as well as set various baselines. Whereas the previous roles are "in the weeds" and focus on pieces and parts of the security program, a security analyst helps define the security program elements and follows through to ensure the elements are being carried out and practiced properly. This person works more at a design level than at an implementation level. Administrative Assistants/Secretaries - This role can be very important to information security; in many companies of smaller size, this may be the individual who greets visitors, signs packages in and out, recognizes individuals who desire to enter the offices, and serves as the phone screener for executives. These individuals may be subject to social engineering attacks, whereby the potential intruder attempts to solicit confidential information that may be used for a subsequent attack. Social engineers prey on

the goodwill of the helpful individual to gain entry. A properly trained assistant will minimize the risk of divulging useful company information or of providing unauthorized entry.
Help Desk Administrator - As the name implies, the help desk is there to field questions from users that report system problems. Problems may include poor response time, potential virus infections, unauthorized access, inability to access system resources, or questions on the use of a program. The help desk is also often where the first indications of security issues and incidents will be seen. A help desk individual would contact the computer security incident response team (CIRT) when a situation meets the criteria developed by the team. The help desk resets passwords, resynchronizes/reinitializes tokens and smart cards, and resolves other problems with access control.
Supervisor - The supervisor role, also called user manager, is ultimately responsible for all user activity and any assets created and owned by these users. For example, suppose Kathy is the supervisor of ten employees. Her responsibilities would include ensuring that these employees understand their responsibilities with respect to security; making sure the employees' account information is up-to-date; and informing the security administrator when an employee is fired, suspended, or transferred. Any change that pertains to an employee's role within the company usually affects what access rights they should and should not have, so the user manager must inform the security administrator of these changes immediately. Change Control Analyst Since the only thing that is constant is change, someone must make sure changes happen securely. The change control analyst is responsible for approving or rejecting requests to make changes to the network, systems, or software. This role must make certain that the change will not introduce any vulnerabilities, that it has been properly tested, and that it is properly rolled out. The change control analyst needs to understand how various changes can affect security, interoperability, performance, and productivity. Or, a company can choose to just roll out the change and see what happens.
The following answers are incorrect:
Systems Administrator - A systems administrator (sysadmin/netadmin) configures network and server hardware and the operating systems to ensure that the information can be available and accessible. The administrator maintains the computing infrastructure using tools and utilities such as patch management and software distribution mechanisms to install updates and test patches on organization computers. The administrator tests and implements system upgrades to ensure the continued reliability of the servers and network devices. The administrator provides vulnerability management through either commercial off the shelf (COTS) and/or non-COTS solutions to test the computing environment and mitigate vulnerabilities appropriately. End User - The end user is responsible for protecting information assets on a daily basis through adherence to the security policies that have been communicated. Security Administrator - A security administrator manages the user access request process and ensures that privileges are provided to those individuals who have been authorized for access by application/system/data owners. This individual has elevated privileges and creates and deletes accounts and access permissions. The security administrator also terminates access privileges when individuals leave their jobs or transfer between company divisions. The security administrator maintains records of access request approvals and produces reports of access rights for the auditor during testing in an access controls audit to demonstrate compliance with the policies.
Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 109
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 108). McGraw-Hill.
Kindle Edition.

QUESTION 294
Which of the following is the MOST important aspect relating to employee termination?

A. The details of employee have been removed from active payroll files.
B. Company property provided to the employee has been returned.
C. User ID and passwords of the employee have been deleted.
D. The appropriate company staff are notified about the termination.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Even though Logical access to information by a terminated employee is possible if the ID and password of the terminated employee has not been deleted this is only one part of the termination procedures. If user ID is not disabled or deleted, it could be possible for the employee without physical access to visit the

companies networks remotely and gain access to the information.

Please note that this can also be seen in a different way: the most important thing to do could also be to inform others of the person's termination, because even if user ID's and passwords are deleted, a terminated individual could simply socially engineer their way back in by calling an individual he/she used to work with and ask them for access. He could intrude on the facility or use other weaknesses to gain access to information after he has been terminated. By notifying the appropriate company staff about the termination, they would in turn intitiate account termination, ask the employee to return company property, and all credentials would be withdrawn for the individual concerned. This answer is more complete than simply disabling account.

It seems harsh and cold when this actually takes place , but too many companies have been hurt by vengeful employees who have lashed out at the company when their positions were revoked for one reason or another. If an employee is disgruntled in any way, or the termination is unfriendly, that employee's accounts should be disabled right away, and all passwords on all systems changed.

For your exam you should know the information below:

Employee Termination Processes

Employees join and leave organizations every day. The reasons vary widely, due to retirement,reduction in force, layoffs, termination with or without cause, relocation to another city, careeropportunities with other employers, or involuntary transfers. Terminations may be friendly or unfriendly and will need different levels of care as a result.

Friendly Terminations

Regular termination is when there is little or no evidence or reason to believe that the termination is not agreeable to both the company and the employee. A standard set of procedures, typically maintained by the human resources department, governs the dismissal of the terminated employee to ensure that company property is returned, and all access is removed. These procedures may include exit interviews and return of keys, identification cards, badges, tokens, and cryptographic keys. Other property, such as laptops, cable locks, credit cards, and phone cards, are also collected. The user manager notifies the security department of the termination to ensure that access is revoked for all platforms and facilities. Some facilities choose to immediately delete the accounts, while others choose to disable the accounts for a policy defined period, for example, 30 days, to account for changes or extensions in the final termination date. The termination process should include a conversation with the departing associate about their continued responsibility for confidentiality of information.

Unfriendly Terminations

Unfriendly terminations may occur when the individual is fired, involuntarily transferred, laid off,or when the organization has reason to believe that the individual has the means and intention to potentially cause harm to the system. Individuals with technical skills and higher levels of access, such as the systems administrators, computer programmers, database administrators, or any individual with elevated privileges, may present higher risk to the environment. These individuals could alter files, plant logic bombs to create system file damage at a future date, or remove sensitive information. Other disgruntled users could enter erroneous data into the system that may not be discovered for several months. In these situations, immediate termination of systems access is warranted at the time of termination or prior to notifying the employee of the termination.

Managing the people aspect of security, from pre-employment to postemployment, is critical to ensure that trustworthy, competent resources are employed to further the business objectives that will protect company information. Each of these actions contributes to preventive, detective, or corrective personnel controls.

The following answers are incorrect:

The other options are less important.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 99

Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 129). McGraw-Hill.
Kindle Edition.

QUESTION 295

Making sure that only those who are supposed to access the data can access is which of the following?

A. confidentiality.

B. capability.

C. integrity.

D. availability.

Correct Answer: A

Explanation

Explanation/Reference:
Explanation: From the published (ISC)2 goals for the Certified Information Systems Security Professional candidate, domain definition. Confidentiality is making sure that only those who are supposed to access the data can access it.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 59.

QUESTION 296
Related to information security, confidentiality is the opposite of which of the following?

A. closure
B. disclosure
C. disposal
D. disaster

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Confidentiality is the opposite of disclosure. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 59.

QUESTION 297
Related to information security, integrity is the opposite of which of the following?

A. abstraction
B. alteration
C. accreditation
D. application

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Integrity is the opposite of "alteration." Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 59.

QUESTION 298
Making sure that the data is accessible when and where it is needed is which of the following?

A. confidentiality
B. integrity
C. acceptability
D. availability

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Availability is making sure that the data is accessible when and where it is needed. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 59.

QUESTION 299

Related to information security, availability is the opposite of which of the following?

A. delegation
B. distribution
C. documentation
D. destruction

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Availability is the opposite of "destruction." Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 59.

QUESTION 300
Related to information security, the prevention of the intentional or unintentional unauthorized disclosure of contents is which of the following?

A. Confidentiality
B. Integrity
C. Availability
D. capability

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Confidentiality is the prevention of the intentional or unintentional unauthorized disclosure of contents.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 60.

QUESTION 301
Related to information security, the guarantee that the message sent is the message received with the assurance that the message was not intentionally or unintentionally altered is an example of which of the following?

A. integrity
B. confidentiality
C. availability
D. identity

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Integrity is the guarantee that the message sent is the message received, and that the message was not intentionally or unintentionally altered. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 60.

QUESTION 302
One of the following assertions is NOT a characteristic of Internet Protocol Security (IPsec)

A. Data cannot be read by unauthorized parties
B. The identity of all IPsec endpoints are confirmed by other endpoints

C. Data is delivered in the exact order in which it is sent
D. The number of packets being exchanged can be counted.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: IPSec provide replay protection that ensures data is not delivered multiple times, however IPsec does not ensure that data is delivered in the exact order in which it is sent. IPSEC uses TCP and packets may be delivered out of order to the receiving side depending which route was taken by the packet.
Internet Protocol Security (IPsec) has emerged as the most commonly used network layer security control for protecting communications. IPsec is a framework of open standards for ensuring private communications over IP networks. Depending on how IPsec is implemented and configured, it can provide any combination of the following types of protection:
Confidentiality. IPsec can ensure that data cannot be read by unauthorized parties. This is accomplished by encrypting data using a cryptographic algorithm and a secret key a value known only to the two parties exchanging data. The data can only be decrypted by someone who has the secret key.
Integrity. IPsec can determine if data has been changed (intentionally or unintentionally) during transit. The integrity of data can be assured by generating a message authentication code (MAC) value, which is a cryptographic checksum of the data. If the data is altered and the MAC is recalculated, the old and new MACs will differ.
Peer Authentication. Each IPsec endpoint confirms the identity of the other IPsec endpoint with which it wishes to communicate, ensuring that the network traffic and data is being sent from the expected host.
Replay Protection. The same data is not delivered multiple times, and data is not delivered grossly out of order. However, IPsec does not ensure that data is delivered in the exact order in which it is sent.
Traffic Analysis Protection. A person monitoring network traffic does not know which parties are communicating, how often communications are occurring, or how much data is being exchanged. However, the number of packets being exchanged can be counted. Access Control. IPsec endpoints can perform filtering to ensure that only authorized IPsec users can access particular network resources. IPsec endpoints can also allow or block certain types of network traffic, such as allowing Web server access but denying file sharing.
The following are incorrect answers because they are all features provided by IPSEC:
"Data cannot be read by unauthorized parties" is wrong because IPsec provides confidentiality through the usage of the Encapsulating Security Protocol (ESP), once encrypted the data cannot be read by unauthorized parties because they have access only to the ciphertext. This is accomplished by encrypting data using a cryptographic algorithm and a session key, a value known only to the two parties exchanging data. The data can only be decrypted by someone who has a copy of the session key.
"The identity of all IPsec endpoints are confirmed by other endpoints" is wrong because IPsec provides peer authentication: Each IPsec endpoint confirms the identity of the other IPsec endpoint with which it wishes to communicate, ensuring that the network traffic and data is being sent from the expected host.
"The number of packets being exchanged can be counted" is wrong because although IPsec provides traffic protection where a person monitoring network traffic does not know which parties are communicating, how often communications are occurring, or how much data is being exchanged, the number of packets being exchanged still can be counted.
Reference(s) used for this question:
NIST 800-77 Guide to IPsec VPNs . Pages 2-3 to 2-4

QUESTION 303
One of these statements about the key elements of a good configuration process is NOT true

A. Accommodate the reuse of proven standards and best practices
B. Ensure that all requirements remain clear, concise, and valid
C. Control modifications to system hardware in order to prevent resource changes
D. Ensure changes, standards, and requirements are communicated promptly and precisely

Correct Answer: C
Explanation

Explanation/Reference:

Explanation: Configuration management isn't about preventing change but ensuring the integrity of IT resources by preventing unauthorised or improper changes. According to the Official ISC2 guide to the CISSP exam, a good CM process is one that can:
(1) accommodate change;
(2) accommodate the reuse of proven standards and best practices; (3) ensure that all requirements remain clear, concise, and valid; (4) ensure changes, standards, and requirements are communicated promptly and precisely; and (5) ensure that the results conform to each instance of the product.
Configuration management
Configuration management (CM) is the detailed recording and updating of information that describes an enterprise's computer systems and networks, including all hardware and software components. Such information typically includes the versions and updates that have been applied to installed software packages and the locations and network addresses of hardware devices. Special configuration management software is available. When a system needs a hardware or software upgrade, a computer technician can accesses the configuration management program and database to see what is currently installed. The technician can then make a more informed decision about the upgrade needed.
An advantage of a configuration management application is that the entire collection of systems can be reviewed to make sure any changes made to one system do not adversely affect any of the other systems
Configuration management is also used in software development, where it is called Unified Configuration Management (UCM). Using UCM, developers can keep track of the source code, documentation, problems, changes requested, and changes made.
Change management
In a computer system environment, change management refers to a systematic approach to keeping track of the details of the system (for example, what operating system release is running on each computer and which fixes have been applied).

QUESTION 304
An area of the Telecommunications and Network Security domain that directly affects the Information Systems Security tenet of Availability can be defined as:

A. Netware availability
B. Network availability
C. Network acceptability
D. Network accountability

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Network availability can be defined as an area of the Telecommunications and Network Security domain that directly affects the Information Systems Security tenet of Availability. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 64.

QUESTION 305
Risk analysis is MOST useful when applied during which phase of the system development process?

A. Project initiation and Planning
B. Functional Requirements definition
C. System Design Specification
D. Development and Implementation

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: In most projects the conditions for failure are established at the beginning of the project. Thus risk management should be established at the commencement of the project with a risk assessment during project

initiation.
As it is clearly stated in the ISC2 book: Security should be included at the first phase of development and throughout all of the phases of the system development life cycle. This is a key concept to understand for the purpose for the exam.
The most useful time is to undertake it at project initiation, although it is often valuable to update the current risk analysis at later stages.
Attempting to retrofit security after the SDLC is completed would cost a lot more money and might be impossible in some cases. Look at the family of browsers we use today, for the past 8 years they always claim that it is the most secure version that has been released and within days vulnerabilities will be found.
Risks should be monitored throughout the SDLC of the project and reassessed when appropriate. The phases of the SDLC can very from one source to another one. It could be as simple as Concept, Design, and Implementation. It could also be expanded to include more phases such as this list proposed within the ISC2 Official Study book:
Project Initiation and Planning
Functional Requirements Definition
System Design Specification
Development and Implementation
Documentations and Common Program Controls
Testing and Evaluation Control, certification and accreditation (C&A) Transition to production (Implementation)
And there are two phases that will extend beyond the SDLC, they are:
Operation and Maintenance Support (O&M)
Revisions and System Replacement (Disposal)
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 291).
and
The Official ISC2 Guide to the CISSP CBK , Second Edition, Page 182-185

QUESTION 306
Which of the following would MOST likely ensure that a system development project meets business objectives?

A. Development and tests are run by different individuals
B. User involvement in system specification and acceptance
C. Development of a project plan identifying all development activities
D. Strict deadlines and budgets

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Effective user involvement is the most critical factor in ensuring that the application meets business objectives.
A great way of getting early input from the user community is by using Prototyping. The prototyping method was formally introduced in the early 1980s to combat the perceived weaknesses of the waterfall model with regard to the speed of development. The objective is to build a simplified version (prototype) of the application, release it for review, and use the feedback from the users' review to build a second, better version. This is repeated until the users are satisfied with the product. t is a four-step process:
initial concept,
design and implement initial prototype,
refine prototype until acceptable, and
complete and release final version.
There is also the Modified Prototype Model (MPM. This is a form of prototyping that is ideal for Web application development. It allows for the basic functionality of a desired system or component to be formally deployed in a quick time frame. The maintenance phase is set to begin after the deployment. The goal is to have the process be flexible enough so the application is not based on the state of the organization at any given time. As the organization grows and the environment changes, the application evolves with it, rather than being frozen in time.

Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 12101-12108 and 12099-12101). Auerbach Publications. Kindle Edition.
and
Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 296).

QUESTION 307
What is RAD?

A. A development methodology

B. A project management technique

C. A measure of system complexity

D. Risk-assessment diagramming

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: RAD stands for Rapid Application Development. RAD is a methodology that enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality. RAD is a programming system that enables programmers to quickly build working programs. In general, RAD systems provide a number of tools to help build graphical user interfaces that would normally take a large development effort.
Two of the most popular RAD systems for Windows are Visual Basic and Delphi. Historically, RAD systems have tended to emphasize reducing development time, sometimes at the expense of generating in-efficient executable code. Nowadays, though, many RAD systems produce extremely faster code that is optimized. Conversely, many traditional programming environments now come with a number of visual tools to aid development. Therefore, the line between RAD systems and other development environments has become blurred.
Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 307)
http://www.webopedia.com

QUESTION 308
Which of the following best describes the purpose of debugging programs?

A. To generate random data that can be used to test programs before implementing them.

B. To ensure that program coding flaws are detected and corrected.

C. To protect, during the programming phase, valid changes from being overwritten by other changes.

D. To compare source code versions before transferring to the test environment

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Debugging provides the basis for the programmer to correct the logic errors in a program under development before it goes into production. Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 298).

QUESTION 309
Which of the following would best describe the difference between white-box testing and black-box testing?

A. White-box testing is performed by an independent programmer team.

B. Black-box testing uses the bottom-up approach.

C. White-box testing examines the program internal logical structure.

D. Black-box testing involves the business units

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Black-box testing observes the system external behavior, while white-box testing is a detailed exam of a logical path, checking the possible conditions. Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 299).

QUESTION 310
Which of the following is a not a preventative control?

A. Deny programmer access to production data.

B. Require change requests to include information about dates, descriptions, cost analysis and anticipated effects.

C. Run a source comparison program between control and current source periodically.

D. Establish procedures for emergency changes.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Running the source comparison program between control and current source periodically allows detection, not prevention, of unauthorized changes in the production environment. Other options are preventive controls.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 309).

QUESTION 311
Which of the following would provide the BEST stress testing environment taking under consideration and avoiding possible data exposure and leaks of sensitive data?

A. Test environment using test data.

B. Test environment using sanitized live workloads data.

C. Production environment using test data.

D. Production environment using sanitized live workloads data.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The best way to properly verify an application or system during a stress test would be to expose it to "live" data that has been sanitized to avoid exposing any sensitive information or Personally Identifiable Data (PII) while in a testing environment. Fabricated test data may not be as varied, complex or computationally demanding as "live" data. A production environment should never be used to test a product, as a production environment is one where the application or system is being put to commercial or operational use. It is a best practice to perform testing in a non-production environment.
Stress testing is carried out to ensure a system can cope with production workloads, but as it may be tested to destruction, a test environment should always be used to avoid damaging the production environment. Hence, testing should never take place in a production environment. If only test data is used, there is no certainty that the system was adequately stress tested.

QUESTION 312
Which of the following BEST explains why computerized information systems frequently fail to meet the needs of users?

A. Inadequate quality assurance (QA) tools.
B. Constantly changing user needs.
C. Inadequate user participation in defining the system's requirements.
D. Inadequate project management.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Inadequate user participation in defining the system's requirements. Most projects fail to meet the needs of the users because there was inadequate input in the initial steps of the project from the user community and what their needs really are. The other answers, while potentially valid, are incorrect because they do not represent the most common problem assosciated with information systems failing to meet the needs of users.
All in One pg 834
Only users can define what their needs are and, therefore, what the system should accomplish. Lack of adequate user involvement, especially in the systems requirements phase, will usually result in a system that doesn't fully or adequately address the needs of the user. Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 296).

QUESTION 313
Which of the following would be the MOST serious risk where a systems development life cycle methodology is inadequate?

A. The project will be completed late.
B. The project will exceed the cost estimates.
C. The project will be incompatible with existing systems.
D. The project will fail to meet business and user needs.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: This is the most serious risk of inadequate systems development life cycle methodolgy.
The following answers are incorrect because :
The project will be completed late is incorrect as it is not most devastating as the above answer. The project will exceed the cost estimates is also incorrect when compared to the above correct answer.
The project will be incompatible with existing systems is also incorrect when compared to the above correct answer.
Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 290).

QUESTION 314
Which of the following is an advantage of prototyping?

A. Prototype systems can provide significant time and cost savings.
B. Change control is often less complicated with prototype systems.
C. It ensures that functions or extras are not added to the intended system.
D. Strong internal controls are easier to implement.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Prototype systems can provide significant time and cost savings, however they also have several disadvantages. They often have poor internal controls, change control becomes much more complicated and it often leads to functions or extras being added to the system that were not originally intended.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 306).

QUESTION 315
Which of the following is a CHARACTERISTIC of a decision support system (DSS) in regards to Threats and Risks Analysis?

A. DSS is aimed at solving highly structured problems.
B. DSS emphasizes flexibility in the decision making approach of users.
C. DSS supports only structured decision-making tasks.
D. DSS combines the use of models with non-traditional data access and retrieval functions.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: DSS emphasizes flexibility in the decision-making approach of users. It is aimed at solving less structured problems, combines the use of models and analytic techniques with traditional data access and retrieval functions and supports semi-structured decision-making tasks.
DSS is sometimes referred to as the Delphi Method or Delphi Technique:
The Delphi technique is a group decision method used to ensure that each member gives an honest opinion of what he or she thinks the result of a particular threat will be. This avoids a group of individuals feeling pressured to go along with others' thought processes and enables them to participate in an independent and anonymous way. Each member of the group provides his or her opinion of a certain threat and turns it in to the team that is performing the analysis. The results are compiled and distributed to the group members, who then write down their comments anonymously and return them to the analysis group. The comments are compiled and redistributed for more comments until a consensus is formed. This method is used to obtain an agreement on cost, loss values, and probabilities of occurrence without individuals having to agree verbally.
Here is the ISC2 book coverage of the subject:
One of the methods that uses consensus relative to valuation of information is the consensus/modified Delphi method. Participants in the valuation exercise are asked to comment anonymously on the task being discussed. This information is collected and disseminated to a participant other than the original author. This participant comments upon the observations of the original author. The information gathered is discussed in a public forum and the best course is agreed upon by the group (consensus).
EXAM TIP:
The DSS is what some of the books are referring to as the Delphi Method or Delphi Technique. Be familiar with both terms for the purpose of the exam.
The other answers are incorrect:
'DSS is aimed at solving highly structured problems' is incorrect because it is aimed at solving less structured problems.
'DSS supports only structured decision-making tasks' is also incorrect as it supports semistructured decision-making tasks.
'DSS combines the use of models with non-traditional data access and retrieval functions' is also incorrect as it combines the use of models and analytic techniques with traditional data access and retrieval functions.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 91). McGraw-Hill. Kindle Edition.
and
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition :
Information Security Governance and Risk Management ((ISC)2 Press) (Kindle Locations 1424- 1426).

Auerbach Publications. Kindle Edition.

QUESTION 316
Which of the following is an advantage in using a bottom-up versus a top-down approach to software testing?

A. Interface errors are detected earlier.
B. Errors in critical modules are detected earlier.
C. Confidence in the system is achieved earlier.
D. Major functions and processing are tested earlier.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The bottom-up approach to software testing begins with the testing of atomic units, such as programs and modules, and work upwards until a complete system testing has taken place. The advantages of using a bottom-up approach to software testing are the fact that there is no need for stubs or drivers and errors in critical modules are found earlier. The other choices refer to advantages of a top down approach which follows the opposite path. Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 299).

QUESTION 317
Which of the following would be the best reason for separating the test and development environments?

A. To restrict access to systems under test.
B. To control the stability of the test environment.
C. To segregate user and development staff.
D. To secure access to systems under development.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The test environment must be controlled and stable in order to ensure that development projects are tested in a realistic environment which, as far as possible, mirrors the live environment.
Reference(s) used for this question:
Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 309).

QUESTION 318
What would BEST define a covert channel?

A. An undocumented backdoor that has been left by a programmer in an operating system
B. An open system port that should be closed.
C. A communication channel that allows transfer of information in a manner that violates the system's security policy.
D. A trojan horse.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The
Answer: A communication channel that allows transfer of information in a manner that violates the system's

security policy.
A covert channel is a way for an entity to receive information in an unauthorized manner. It is an information flow that is not controlled by a security mechanism. This type of information path was not developed for communication; thus, the system does not properly protect this path, because the developers never envisioned information being passed in this way. Receiving information in this manner clearly violates the system's security policy. The channel to transfer this unauthorized data is the result of one of the following conditions:· Oversight in the development of the product
· Improper implementation of access controls
· Existence of a shared resource between the two entities · Installation of a Trojan horse
The following answers are incorrect:
An undocumented backdoor that has been left by a programmer in an operating system is incorrect because it is not a means by which unauthorized transfer of information takes place. Such backdoor is usually referred to as a Maintenance Hook. An open system port that should be closed is incorrect as it does not define a covert channel. A trojan horse is incorrect because it is a program that looks like a useful program but when you install it it would include a bonus such as a Worm, Backdoor, or some other malware without the installer knowing about it.
Reference(s) used for this question:
Shon Harris AIO v3 , Chapter-5 : Security Models & Architecture AIOv4 Security Architecture and Design (pages 343 - 344) AIOv5 Security Architecture and Design (pages 345 - 346)

QUESTION 319
Which of the following is NOT an administrative control?

A. Logical access control mechanisms
B. Screening of personnel
C. Development of policies, standards, procedures and guidelines
D. Change control procedures

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: It is considered to be a technical control. Logical is synonymous with Technical Control. That was the easy answer. There are three broad categories of access control: Administrative, Technical, and Physical. Each category has different access control mechanisms that can be carried out manually or automatically. All of these access control mechanisms should work in concert with each other to protect an infrastructure and its data.
Each category of access control has several components that fall within it, as shown here:
Administrative Controls
· Policy and procedures
· Personnel controls
· Supervisory structure
· Security-awareness training
· Testing
Physical Controls
Network segregation
Perimeter security
Computer controls
Work area separation
Data backups
Technical Controls
System access
Network architecture
Network access
Encryption and protocols
Control zone
Auditing
The following answers are incorrect :

Screening of personnel is considered to be an administrative control Development of policies, standards, procedures and guidelines is considered to be an administrative control
Change control procedures is considered to be an administrative control. Reference : Shon Harris AIO v3 , Chapter - 3 : Security Management Practices , Page : 52-54

QUESTION 320
Which of the following is NOT a technical control?

A. Password and resource management
B. Identification and authentication methods
C. Monitoring for physical intrusion
D. Intrusion Detection Systems

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: It is considered to be a 'Physical Control' There are three broad categories of access control: administrative, technical, and physical. Each category has different access control mechanisms that can be carried out manually or automatically. All of these access control mechanisms should work in concert with each other to protect an infrastructure and its data.
Each category of access control has several components that fall within it, a partial list is shown here. Not all controls fall into a single category, many of the controls will be in two or more categories. Below you have an example with backups where it is in all three categories:
Administrative Controls
Policy and procedures
- A backup policy would be in place
Personnel controls
Supervisory structure
Security-awareness training
Testing
Physical Controls
Network segregation
Perimeter security
Computer controls
Work area separation
Data backups (actual storage of the media, i:e Offsite Storage Facility) Cabling
Technical Controls
System access
Network architecture
Network access
Encryption and protocols
Control zone
Auditing
Backup (Actual software doing the backups)
The following answers are incorrect :
Password and resource management is considered to be a logical or technical control. Identification and authentication methods is considered to be a logical or technical control. Intrusion Detection Systems is considered to be a logical or technical control. Reference : Shon Harris , AIO v3 , Chapter - 4 : Access Control , Page : 180 - 185

QUESTION 321
Which of the following is BEST defined as a physical control?

A. Monitoring of system activity
B. Fencing
C. Identification and authentication methods

D. Logical access control mechanisms

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Physical controls are items put into place to protect facility, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting.
The following answers are incorrect answers:
Monitoring of system activity is considered to be administrative control. Identification and authentication methods are considered to be a technical control. Logical access control mechanisms is also considered to be a technical control.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 1280- 1282). McGraw-Hill. Kindle Edition.

QUESTION 322
Which of the following is given the responsibility of the maintenance and protection of the data?

A. Data owner
B. Data custodian
C. User
D. Security administrator

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: It is usually responsible for maintaining and protecting the data.
The following answers are incorrect:
Data owner is usually a member of management , in charge of a specific business unit and is ultimately responsible for the protection and use of the information. User is any individual who routinely uses the data for work-related tasks. Security administrator's tasks include creating new system user accounts , implementing new security software.
References : Shon Harris AIO v3 , Chapter - 3: Security Management Practices , Pages : 99 - 103

QUESTION 323
Who should DECIDE how a company should approach security and what security measures should be implemented?

A. Senior management
B. Data owner
C. Auditor
D. The information security specialist

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: They are responsible for security of the organization and the protection of its assets.
The following answers are incorrect because :
Data owner is incorrect as data owners should not decide as to what security measures should be applied. Auditor is also incorrect as auditor cannot decide as to what security measures should be applied. The information security specialist is also incorrect as they may have the technical knowledge of how security measures should be implemented and configured , but they should not be in a position of deciding what measures should be applied.
Reference : Shon Harris AIO v3 , Chapter-3: Security Management Practices , Page : 51.

QUESTION 324
Which of the following is responsible for MOST of the security issues?

A. Outside espionage
B. Hackers
C. Personnel
D. Equipment failure

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Personnel cause more security issues than hacker attacks, outside espionage, or equipment failure.
The following answers are incorrect because:
Outside espionage is incorrect as it is not the best answer. Hackers is also incorrect as it is not the best answer. Equipment failure is also incorrect as it is not the best answer. Reference : Shon Harris AIO v3 , Chapter-3: Security Management Practices , Page : 56

QUESTION 325
What are the three FUNDAMENTAL principles of security?

A. Accountability, confidentiality and integrity
B. Confidentiality, integrity and availability
C. Integrity, availability and accountability
D. Availability, accountability and confidentiality

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The following answers are incorrect because:
Accountability, confidentiality and integrity is not the correct answer as Accountability is not one of the fundamental principle of security.
Integrity, availability and accountability is not the correct answer as Accountability is not one of the fundamental principle of security.
Availability, accountability and confidentiality is not the correct answer as Accountability is not one of the fundamental objective of security.
References : Shon Harris AIO v3 , Chapter - 3: Security Management Practices , Pages : 49-52

QUESTION 326
Within the context of the CBK, which of the following provides a MINIMUM level of security ACCEPTABLE for an environment ?

A. A baseline
B. A standard
C. A procedure
D. A guideline

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Baselines provide the minimum level of security necessary throughout the organization.
Standards specify how hardware and software products should be used throughout the organization.

Procedures are detailed step-by-step instruction on how to achieve certain tasks. Guidelines are recommendation actions and operational guides to personnel when a specific standard does not apply.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 3: Security Management Practices (page 94).

QUESTION 327
According to private sector data classification levels, how would salary levels and medical information be classified?

A. Public.
B. Internal Use Only.
C. Restricted.
D. Confidential.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Typically there are three to four levels of information classification used by most organizations:
Confidential: Information that, if released or disclosed outside of the organization, would create severe problems for the organization. For example, information that provides a competitive advantage is important to the technical or financial success (like trade secrets, intellectual property, or research designs), or protects the privacy of individuals would be considered confidential. Information may include payroll information, health records, credit information, formulas, technical designs, restricted regulatory information, senior management internal correspondence, or business strategies or plans. These may also be called top secret, privileged, personal, sensitive, or highly confidential. In other words this information is ok within a defined group in the company such as marketing or sales, but is not suited for release to anyone else in the company without permission.
The following answers are incorrect:
Public: Information that may be disclosed to the general public without concern for harming the company, employees, or business partners. No special protections are required, and information in this category is sometimes referred to as unclassified. For example, information that is posted to a company's public Internet site, publicly released announcements, marketing materials, cafeteria menus, and any internal documents that would not present harm to the company if they were disclosed would be classified as public. While there is little concern for confidentiality, integrity and availability should be considered.
Internal Use Only: Information that could be disclosed within the company, but could harm the company if disclosed externally. Information such as customer lists, vendor pricing, organizational policies, standards and procedures, and internal organization announcements would need baseline security protections, but do not rise to the level of protection as confidential information. In other words, the information may be used freely within the company but any unapproved use outside the company can pose a chance of harm.
Restricted: Information that requires the utmost protection or, if discovered by unauthorized personnel, would cause irreparable harm to the organization would have the highest level of classification. There may be very few pieces of information like this within an organization, but data classified at this level requires all the access control and protection mechanisms available to the organization. Even when information classified at this level exists, there will be few copies of it Reference(s) Used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 952-976). Auerbach Publications. Kindle Edition.

QUESTION 328
Which of the following would be the best criterion to consider in determining the classification of an information asset?

A. Value
B. Age
C. Useful life
D. Personal association

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Information classification should be based on the value of the information to the organization and its sensitivity (reflection of how much damage would accrue due to disclosure). Age is incorrect. While age might be a consideration in some cases, the guiding principles should be value and sensitivity.
Useful life. While useful lifetime is relevant to how long data protections should be applied, the classification is based on information value and sensitivity. Personal association is incorrect. Information classification decisions should be based on value of the information and its sensitiviry.
References
CBK, pp. 101 - 102.

QUESTION 329
Which of the following is not a responsibility of an information (data) owner?

A. Determine what level of classification the information requires.
B. Periodically review the classification assignments against business needs.
C. Delegate the responsibility of data protection to data custodians.
D. Running regular backups and periodically testing the validity of the backup data.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: This responsibility would be delegated to a data custodian rather than being performed directly by the information owner.
"Determine what level of classification the information requires" is incorrect. This is one of the major responsibilities of an information owner.
"Periodically review the classification assignments against business needs" is incorrect. This is one of the major responsibilities of an information owner. "Delegates responsibility of maintenance of the data protection mechanisms to the data custodian" is incorrect. This is a responsibility of the information owner.

CBK p. 105.
AIO3, p. 53-54, 960

QUESTION 330
Which of the following embodies all the detailed actions that personnel are required to follow?

A. Standards
B. Guidelines
C. Procedures
D. Baselines

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Procedures are step-by-step instructions in support of of the policies, standards, guidelines and baselines. The procedure indicates how the policy will be implemented and who does what to accomplish the tasks."
Standards is incorrect. Standards are a "Mandatory statement of minimum requirements that support some part of a policy, the standards in this case is your own company standards and not standards such as the ISO standards"
Guidelines is incorrect. "Guidelines are discretionary or optional controls used to enable individuals to make judgments with respect to security actions." Baselines is incorrect. Baselines "are a minimum acceptable level of security. This minimum is implemented using specific rules necessary to implement the security controls in

support of the policy and standards." For example, requiring a password of at leat 8 character would be an example. Requiring all users to have a minimun of an antivirus, a personal firewall, and an anti spyware tool could be another example.
CBK, pp. 12 - 16. Note especially the discussion of the "hammer policy" on pp. 16-17 for the differences between policy, standard, guideline and procedure.
AIO3, pp. 88-93.

QUESTION 331
Which of the following choices describe a condition when RAM and Secondary storage are used together?

A. Primary storage
B. Secondary storage
C. Virtual storage
D. Real storage

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Virtual storage a service provided by the operating system where it uses a combination of RAM and disk storage to simulate a much larger address space than is actually present. Infrequently used portions of memory are paged out by being written to secondary storage and paged back in when required by a running program. Most OS's have the ability to simulate having more main memory than is physically available in the system. This is done by storing part of the data on secondary storage, such as a disk. This can be considered a virtual page. If the data requested by the system is not currently in main memory, a page fault is taken. This condition triggers the OS handler. If the virtual address is a valid one, the OS will locate the physical page, put the right information in that page, update the translation table, and then try the request again. Some other page might be swapped out to make room. Each process may have its own separate virtual address space along with its own mappings and protections.
The following are incorrect answers:
Primary storage is incorrect. Primary storage refers to the combination of RAM, cache and the processor registers. Primary Storage The data waits for processing by the processors, it sits in a staging area called primary storage. Whether implemented as memory, cache, or registers (part of the CPU), and regardless of its location, primary storage stores data that has a high probability of being requested by the CPU, so it is usually faster than long-term, secondary storage. The location where data is stored is denoted by its physical memory address. This memory register identifier remains constant and is independent of the value stored there. Some examples of primary storage devices include random-access memory (RAM), synchronous dynamic randomaccess memory (SDRAM), and read-only memory (ROM). RAM is volatile, that is, when the system shuts down, it flushes the data in RAM although recent research has shown that data may still be retrievable.
Contrast this
Secondary storage is incorrect. Secondary storage holds data not currently being used by the CPU and is used when data must be stored for an extended period of time using high-capacity, nonvolatile storage. Secondary storage includes disk, floppies, CD's, tape, etc. While secondary storage includes basically anything different from primary storage, virtual memory's use of secondary storage is usually confined to high-speed disk storage. Real storage is incorrect. Real storage is another word for primary storage and distinguishes physical memory from virtual memory.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, ThirdEdition ((ISC)2 Press) (Kindle Locations 17164-17171). Auerbach Publications. Kindle Edition. Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, ThirdEdition ((ISC)2 Press) (Kindle Locations 17196-17201). Auerbach Publications. Kindle Edition. Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, ThirdEdition ((ISC)2 Press) (Kindle Locations 17186-17187). Auerbach Publications. Kindle Edition.

QUESTION 332
Which of the following statements pertaining to protection rings is false?

A. They provide strict boundaries and definitions on what the processes that work within each ring can access.

B. Programs operating in inner rings are usually referred to as existing in a privileged mode.
C. They support the CIA triad requirements of multitasking operating systems.
D. They provide users with a direct access to peripherals

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: In computer science, hierarchical protection domains, often called protection rings, are mechanisms to protect data and functionality from faults (fault tolerance) and malicious behaviour (computer security). This approach is diametrically opposite to that of capability-based security.
Computer operating systems provide different levels of access to resources. A protection ring is one of two or more hierarchical levels or layers of privilege within the architecture of a computer system. This is generally hardware-enforced by some CPU architectures that provide different CPU modes at the hardware or microcode level.
Rings are arranged in a hierarchy from most privileged (most trusted, usually numbered zero) to least privileged (least trusted, usually with the highest ring number). On most operating systems, Ring 0 is the level with the most privileges and interacts most directly with the physical hardware such as the CPU and memory.
Special gates between rings are provided to allow an outer ring to access an inner ring's resources in a predefined manner, as opposed to allowing arbitrary usage. Correctly gating access between rings can improve security by preventing programs from one ring or privilege level from misusing resources intended for programs in another. For example, spyware running as a user program in Ring 3 should be prevented from turning on a web camera without informing the user, since hardware access should be a Ring 1 function reserved for device drivers. Programs such as web browsers running in higher numbered rings must request access to the network, a resource restricted to a lower numbered ring.
"They provide strict boundaries and definitions on what the processes that work within each ring can access" is incorrect. This is in fact one of the characteristics of a ring protection system. "Programs operating in inner rings are usually referred to as existing in a privileged mode" is incorrect. This is in fact one of the characteristics of a ring protection system. "They support the CIA triad requirements of multitasking operating systems" is incorrect. This is in fact one of the characteristics of a ring protection system.
Reference(s) used for this question:
CBK, pp. 310-311
AIO3, pp. 253-256
AIOv4 Security Architecture and Design (pages 308 - 310) AIOv5 Security Architecture and Design (pages 309 - 312)

QUESTION 333
What is it called when a computer uses more than one CPU in parallel to execute instructions?

A. Multiprocessing
B. Multitasking
C. Multithreading
D. Parallel running

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: A system with multiple processors is called a multiprocessing system. Multitasking is incorrect. Multitasking involves sharing the processor amoung all ready processes. Though it appears to the user that multiple processes are executing at the same time, only one process is running at any point in time. Multithreading is incorrect. The developer can structure a program as a collection of independent threads to achieve better concurrency. For example, one thread of a program might be performing a calculation while another is waiting for additional input from the user. "Parallel running" is incorrect. This is not a real term and is just a distraction.

CBK, pp. 315-316
AIO3, pp. 234 - 239

QUESTION 334
What can be defined as an abstract machine that mediates all access to objects by subjects to ensure that subjects have the necessary access rights and to protect objects from unauthorized access?

A. The Reference Monitor
B. The Security Kernel
C. The Trusted Computing Base
D. The Security Domain

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The reference monitor refers to abstract machine that mediates all access to objects by subjects. This question is asking for the concept that governs access by subjects to objects, thus the reference monitor is the best answer. While the security kernel is similar in nature, it is what actually enforces the concepts outlined in the reference monitor. In operating systems architecture a reference monitor concept defines a set of design requirements on a reference validation mechanism, which enforces an access control policy over subjects' (e.g., processes and users) ability to perform operations (e.g., read and write) on objects (e.g., files and sockets) on a system. The properties of a reference monitor are:
The reference validation mechanism must always be invoked (complete mediation). Without this property, it is possible for an attacker to bypass the mechanism and violate the security policy. The reference validation mechanism must be tamperproof (tamperproof). Without this property, an attacker can undermine the mechanism itself so that the security policy is not correctly enforced. The reference validation mechanism must be small enough to be subject to analysis and tests, the completeness of which can be assured (verifiable). Without this property, the mechanism might be flawed in such a way that the policy is not enforced.
For example, Windows 3.x and 9x operating systems were not built with a reference monitor, whereas the Windows NT line, which also includes Windows 2000 and Windows XP, was designed to contain a reference monitor, although it is not clear that its properties (tamperproof, etc.) have ever been independently verified, or what level of computer security it was intended to provide.
The claim is that a reference validation mechanism that satisfies the reference monitor concept will correctly enforce a system's access control policy, as it must be invoked to mediate all securitysensitive operations, must not be tampered, and has undergone complete analysis and testing to verify correctness. The abstract model of a reference monitor has been widely applied to any type of system that needs to enforce access control, and is considered to express the necessary and sufficient properties for any system making this security claim. According to Ross Anderson, the reference monitor concept was introduced by James Anderson in an influential 1972 paper.
Systems evaluated at B3 and above by the Trusted Computer System Evaluation Criteria (TCSEC) must enforce the reference monitor concept.
The reference monitor, as defined in AIO V5 (Harris) is: "an access control concept that refers to an abstract machine that mediates all access to objects by subjects." The security kernel, as defined in AIO V5 (Harris) is: "the hardware, firmware, and software elements of a trusted computing based (TCB) that implement the reference monitor concept. The kernel must mediate all access between subjects and objects, be protected from modification, and be verifiable as correct."
The trusted computing based (TCB), as defined in AIO V5 (Harris) is: "all of the protection mechanisms within a computer system (software, hardware, and firmware) that are responsible for enforcing a security policy."
The security domain, "builds upon the definition of domain (a set of resources available to a subject) by adding the fact that resources withing this logical structure (domain) are working under the same security policy and managed by the same group." The following answers are incorrect:
"The security kernel" is incorrect. One of the places a reference monitor could be implemented is in the security kernel but this is not the best answer. "The trusted computing base" is incorrect. The reference monitor is an important concept in the TCB but this is not the best answer.
"The security domain is incorrect." The reference monitor is an important concept in the security domain but this is not the best answer.
Reference(s) used for this question:

Official ISC2 Guide to the CBK, page 324
AIO Version 3, pp. 272 - 274
AIOv4 Security Architecture and Design (pages 327 - 328) AIOv5 Security Architecture and Design (pages 330 - 331) Wikipedia article at https://en.wikipedia.org/wiki/Reference_monitor

QUESTION 335
Which of the following is not a method to protect objects and the data within the objects?

A. Layering
B. Data mining
C. Abstraction
D. Data hiding

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Data mining is used to reveal hidden relationships, patterns and trends by running queries on large data stores.
Data mining is the act of collecting and analyzing large quantities of information to determine patterns of use or behavior and use those patterns to form conclusions about past, current, or future behavior. Data mining is typically used by large organizations with large databases of customer or consumer behavior. Retail and credit companies will use data mining to identify buying patterns or trends in geographies, age groups, products, or services. Data mining is essentially the statistical analysis of general information in the absence of specific data.
The following are incorrect answers:
They are incorrect as they all apply to Protecting Objects and the data within them. Layering, abstraction and data hiding are related concepts that can work together to produce modular software that implements an organizations security policies and is more reliable in operation. Layering is incorrect. Layering assigns specific functions to each layer and communication between layers is only possible through well-defined interfaces. This helps preclude tampering in violation of security policy. In computer programming, layering is the organization of programming into separate functional components that interact in some sequential and hierarchical way, with each layer usually having an interface only to the layer above it and the layer below it. Abstraction is incorrect. Abstraction "hides" the particulars of how an object functions or stores information and requires the object to be manipulated through well-defined interfaces that can be designed to enforce security policy. Abstraction involves the removal of characteristics from an entity in order to easily represent its essential properties. Data hiding is incorrect. Data hiding conceals the details of information storage and manipulation within an object by only exposing well defined interfaces to the information rather than the information itslef. For example, the details of how passwords are stored could be hidden inside a password object with exposed interfaces such as check_password, set_password, etc. When a password needs to be verified, the test password is passed to the check_password method and a boolean (true/false) result is returned to indicate if the password is correct without revealing any details of how/where the real passwords are stored. Data hiding maintains activities at different security levels to separate these levels from each other.
The following reference(s) were used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 27535-27540). Auerbach Publications. Kindle Edition.
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 4269-4273). Auerbach Publications. Kindle Edition.

QUESTION 336
What is called the formal acceptance of the adequacy of a system's overall security by the management?

A. Certification
B. Acceptance
C. Accreditation
D. Evaluation

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Accreditation is the authorization by management to implement software or systems in a production environment. This authorization may be either provisional or full.
The following are incorrect answers:
Certification is incorrect. Certification is the process of evaluating the security stance of the software or system against a selected set of standards or policies. Certification is the technical evaluation of a product. This may precede accreditation but is not a required precursor. Acceptance is incorrect. This term is sometimes used as the recognition that a piece of software or system has met a set of functional or service level criteria (the new payroll system has passed its acceptance test). Certification is the better tem in this context. Evaluation is incorrect. Evaluation is certainly a part of the certification process but it is not the best answer to the question.
Reference(s) used for this question:
The Official Study Guide to the CBK from ISC2, pages 559-560 AIO3, pp. 314 - 317
AIOv4 Security Architecture and Design (pages 369 - 372) AIOv5 Security Architecture and Design (pages 370 - 372)

QUESTION 337
Which property ensures that only the intended recipient can access the data and nobody else?

A. Confidentiality
B. Capability
C. Integrity
D. Availability

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Confidentiality is defined as the property that ensures that only the intended recipient can access the data and nobody else. It is usually achieve using cryptogrphic methods, tools, and protocols.
Confidentiality supports the principle of "least privilege" by providing that only authorized individuals, processes, or systems should have access to information on a need-to-know basis. The level of access that an authorized individual should have is at the level necessary for them to do their job. In recent years, much press has been dedicated to the privacy of information and the need to protect it from individuals, who may be able to commit crimes by viewing the information. Identity theft is the act of assuming one's identity through knowledge of confidential information obtained from various sources.
The following are incorrect answers:
Capability is incorrect. Capability is relevant to access control. Capability-based security is a concept in the design of secure computing systems, one of the existing security models. A capability (known in some systems as a key) is a communicable, unforgeable token of authority. It refers to a value that references an object along with an associated set of access rights. A user program on a capability-based operating system must use a capability to access an object. Capability-based security refers to the principle of designing user programs such that they directly share capabilities with each other according to the principle of least privilege, and to the operating system infrastructure necessary to make such transactions efficient and secure. Integrity is incorrect. Integrity protects information from unauthorized modification or loss. Availability is incorrect. Availability assures that information and services are available for use by authorized entities according to the service level objective.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 9345-9349). Auerbach Publications. Kindle Edition. http://en.wikipedia.org/wiki/Capability-based_security

QUESTION 338
Making sure that the data has not been changed unintentionally, due to an accident or malice is:

A. Integrity.
B. Confidentiality.
C. Availability.
D. Auditability.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Integrity refers to the protection of information from unauthorized modification or deletion. Confidentiality is incorrect. Confidentiality refers to the protection of information from unauthorized disclosure. Availability is incorrect. Availability refers to the assurance that information and services will be available to authorized users in accordance with the service level objective. Auditability is incorrect. Auditability refers to the ability to trace an action to the identity that performed it and identify the date and time at which it occurred.

CBK, pp. 5 - 6
AIO3, pp. 56 - 57

QUESTION 339
Which of the following are the steps usually followed in the development of documents such as security policy, standards and procedures?

A. design, development, publication, coding, and testing.
B. design, evaluation, approval, publication, and implementation.
C. initiation, evaluation, development, approval, publication, implementation, and maintenance.
D. feasibility, development, approval, implementation, and integration.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The common steps used the the development of security policy are initiation of the project, evaluation, development, approval, publication, implementation, and maintenance. The other choices listed are the phases of the software development life cycle and not the step used to develop ducuments such as Policies, Standards, etc...
TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 3, 2002, Auerbach Publications.

QUESTION 340
What is the goal of the Maintenance phase in a common development process of a security policy?

A. to review the document on the specified review date
B. publication within the organization
C. to write a proposal to management that states the objectives of the policy
D. to present the document to an approving body

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: "publication within the organization" is the goal of the Publication Phase "write a proposal to management that states the objectives of the policy" is part of Initial and Evaluation Phase "Present the document to an approving body" is part of Approval Phase. TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 3, 2002, Auerbach Publications.
Also: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery

Planning (page 286).

QUESTION 341
What is the difference between Advisory and Regulatory security policies?

A. there is no difference between them
B. regulatory policies are high level policy, while advisory policies are very detailed
C. Advisory policies are not mandated. Regulatory policies must be implemented.
D. Advisory policies are mandated while Regulatory policies are not

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Advisory policies are security polices that are not mandated to be followed but are strongly suggested, perhaps with serious consequences defined for failure to follow them (such as termination, a job action warning, and so forth). A company with such policies wants most employees to consider these policies mandatory.
Most policies fall under this broad category.
Advisory policies can have many exclusions or application levels. Thus, these policies can control some employees more than others, according to their roles and responsibilities within that organization. For example, a policy that
requires a certain procedure for transaction processing might allow for an alternative procedure under certain, specified conditions.
Regulatory
Regulatory policies are security policies that an organization must implement due to compliance, regulation, or other legal requirements. These companies might be financial institutions, public utilities, or some other type of organization that operates in the public interest. These policies are usually very detailed and are specific to the industry in which the organization operates.
Regulatory polices commonly have two main purposes:
1. To ensure that an organization is following the standard procedures or base practicesof operation in its specific industry
2. To give an organization the confidence that it is following the standard and accepted industry policy
Informative
Informative policies are policies that exist simply to inform the reader. There are no implied or specified requirements, and the audience for this information could be certain internal (within the organization) or external parties. This does not mean that the policies are authorized for public consumption but that they are general enough to be distributed to external parties (vendors accessing an extranet, for example) without a loss of confidentiality.

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Page 12, Chapter 1: Security Management Practices.
also see:
The CISSP Prep Guide:Mastering the Ten Domains of Computer Security by Ronald L. Krutz, Russell Dean Vines, Edward M. Stroz
also see:
http://i-data-recovery.com/information-security/information-security-policies-standards-guidelinesand-procedures

QUESTION 342
What is the main purpose of Corporate Security Policy?

A. To transfer the responsibility for the information security to all users of the organization
B. To communicate management's intentions in regards to information security
C. To provide detailed steps for performing specific actions
D. To provide a common framework for all development activities

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: A Corporate Security Policy is a high level document that indicates what are management`s intentions in regard to Information Security within the organization. It is high level in purpose, it does not give you details about specific products that would be use, specific steps, etc..
The organization's requirements for access control should be defined and documented in its security policies. Access rules and rights for each user or group of users should be clearly stated in an access policy statement. The access control policy should minimally consider:
Statements of general security principles and their applicability to the organization Security requirements of individual enterprise applications, systems, and services Consistency between the access control and information classification policies of different systems and networks
Contractual obligations or regulatory compliance regarding protection of assets Standards defining user access profiles for organizational roles Details regarding the management of the access control system As a Certified Information System Security Professional (CISSP) you would be involved directly in the drafting and coordination of security policies, standards and supporting guidelines, procedures, and baselines.
Guidance provided by the CISSP for technical security issues, and emerging threats are considered for the adoption of new policies. Activities such as interpretation of government regulations and industry trends and analysis of vendor solutions to include in the security architecture that advances the security of the organization are performed by the CISSP as well.
The following are incorrect answers:
To transfer the responsibility for the information security to all users of the organization is bogus. You CANNOT transfer responsibility, you can only tranfer authority. Responsibility will also sit with upper management. The keyworks ALL and USERS is also an indication that it is the wrong choice.
To provide detailed steps for performing specific actions is also a bogus detractor. A step by step document is referred to as a procedure. It details how to accomplish a specific task. To provide a common framework for all development activities is also an invalid choice. Security Policies are not restricted only to development activities.
Reference Used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 1551-1565). Auerbach Publications. Kindle Edition.
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 9109-9112). Auerbach Publications. Kindle Edition.

QUESTION 343
Which of the following is not a component of a Operations Security "triples"?

A. Asset
B. Threat
C. Vulnerability
D. Risk

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The Operations Security domain is concerned with triples - threats, vulnerabilities and assets.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 216.

QUESTION 344
When two or more separate entities (usually persons) operating in concert to protect sensitive functions or information must combine their knowledge to gain access to an asset, this is known as?

A. Dual Control

B. Need to know
C. Separation of duties
D. Segragation of duties

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The question mentions clearly "operating together". Which means the BEST answer is Dual Control.
Two mechanisms necessary to implement high integrity environments where separation of duties is paramount are dual control or split knowledge.
Dual control enforces the concept of keeping a duo responsible for an activity. It requires more than one employee available to perform a task. It utilizes two or more separate entities (usually persons), operating together, to protect sensitive functions or information. Whenever the dual control feature is limited to something you know., it is often called split knowledge (such as part of the password, cryptographic keys etc.) Split knowledge is the unique "what each must bring" and joined together when implementing dual control. To illustrate, let say you have a box containing petty cash is secured by one combination lock and one keyed lock. One employee is given the combination to the combo lock and another employee has possession of the correct key to the keyed lock. In order to get the cash out of the box both employees must be present at the cash box at the same time. One cannot open the box without the other. This is the aspect of dual control.
On the other hand, split knowledge is exemplified here by the different objects (the combination to the combo lock and the correct physical key), both of which are unique and necessary, that each brings to the meeting.
This is typically used in high value transactions / activities (as per the organizations risk appetite) such as:
Approving a high value transaction using a special user account, where the password of this user account is split into two and managed by two different staff. Both staff should be present to enter the password for a high value transaction. This is often combined with the separation of duties principle. In this case, the posting of the transaction would have been performed by another staff. This leads to a situation where collusion of at least 3 people are required to make a fraud transaction which is of high value.
Payment Card and PIN printing is separated by SOD principles. Now the organization can even enhance the control mechanism by implementing dual control / split knowledge. The card printing activity can be modified to require two staff to key in the passwords for initiating the printing process. Similarly, PIN printing authentication can also be made to be implemented with dual control. Many Host Security modules (HSM) comes with built in controls for dual controls where physical keys are required to initiate the PIN printing process. Managing encryption keys is another key area where dual control / split knowledge to be implemented.
PCI DSS defines Dual Control as below. This is more from a cryptographic perspective, still useful:
Dual Control: Process of using two or more separate entities (usually persons) operating in concert to protect sensitive functions or information. Both entities are equally responsible for the physical protection of materials involved in vulnerable transactions. No single person is permitted to access or use the materials (for example, the cryptographic key). For manual key generation, conveyance, loading, storage, and retrieval, dual control requires dividing knowledge of the key among the entities. (See also Split Knowledge).
Split knowledge: Condition in which two or more entities separately have key components that individually convey no knowledge of the resultant cryptographic key. It is key for information security professionals to understand the differences between Dual Control and Separation of Duties. Both complement each other, but are not the same.
The following were incorrect answers:
Segregation of Duties address the splitting of various functions within a process to different users so that it will not create an opportunity for a single user to perform conflicting tasks. For example, the participation of two or more persons in a transaction creates a system of checks and balances and reduces the possibility of fraud considerably. So it is important for an organization to ensure that all tasks within a process has adequate separation. Let us look at some use cases of segregation of duties A person handling cash should not post to the accounting records A loan officer should not disburse loan proceeds for loans they approved Those who have authority to sign cheques should not reconcile the bank accounts The credit card printing personal should not print the credit card PINs Customer address changes must be verified by a second employee before the change can be activated.
In situations where the separation of duties are not possible, because of lack of staff, the senior management should set up additional measure to offset the lack of adequate controls. To summarise, Segregation of Duties is about Separating the conflicting duties to reduce fraud in an end to end function.

Need To Know (NTK):
The term "need to know", when used by government and other organizations (particularly those related to the military), describes the restriction of data which is considered very sensitive. Under need-to-know restrictions, even if one has all the necessary official approvals (such as a security clearance) to access certain information, one would not be given access to such information, unless one has a specific need to know; that is, access to the information must be necessary for the conduct of one's official duties. As with most security mechanisms, the aim is to make it difficult for unauthorized access to occur, without inconveniencing legitimate access. Need-toknow also aims to discourage "browsing" of sensitive material by limiting access to the smallest possible number of people.
EXAM TIP: HOW TO DECIPHER THIS question
First, you probably nototiced that both Separation of Duties and Segregation of Duties are synonymous with each others. This means they are not the BEST answers for sure. That was an easy first step.
For the exam remember:
Separation of Duties is synonymous with Segregation of Duties Dual Control is synonymous with Split Knowledge
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 16048-16078). Auerbach Publications. Kindle Edition.
and
http://www.ciso.in/dual-control-or-segregation-of-duties/

QUESTION 345
Which of the following is NOT a proper component of Media Viability Controls?

A. Storage
B. Writing
C. Handling
D. Marking

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Media Viability Controls include marking, handling and storage. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 231.

QUESTION 346
A channel within a computer system or network that is designed for the authorized transfer of information is identified as a(n)?

A. Covert channel
B. Overt channel
C. Opened channel
D. Closed channel

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: An overt channel is a path within a computer system or network that is designed for the authorized transfer of data. The opposite would be a covert channel which is an unauthorized path.
A covert channel is a way for an entity to receive information in an unauthorized manner. It is an information flow that is not controlled by a security mechanism. This type of information path was not developed for communication; thus, the system does not properly protect this path, because the developers never envisioned information being passed in this way. Receiving information in this manner clearly violates the system's security policy.

All of the other choices are bogus detractors.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 219.
and
Shon Harris, CISSP All In One (AIO), 6th Edition , page 380 and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 378). McGraw-Hill.
Kindle Edition.

QUESTION 347
When attempting to establish Liability, which of the following would be describe as performing the ongoing maintenance necessary to keep something in proper working order, updated, effective, or to abide by what is commonly expected in a situation?

A. Due care
B. Due concern
C. Due diligence
D. Due practice

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: My friend JD Murray at Techexams.net has a nice definition of both, see his explanation below:
Oh, I hate these two. It's like describing the difference between "jealously" and "envy." Kinda the same thing but not exactly. Here it goes:
Due diligence is performing reasonable examination and research before committing to a course of action. Basically, "look before you leap." In law, you would perform due diligence by researching the terms of a contract before signing it. The opposite of due diligence might be "haphazard" or "not doing your homework."
Due care is performing the ongoing maintenance necessary to keep something in proper working order, or to abide by what is commonly expected in a situation. This is especially important if the due care situation exists because of a contract, regulation, or law. The opposite of due care is "negligence."
In summary, Due Diligence is Identifying threats and risks while Due Care is Acting upon findings to mitigate risks
EXAM TIP:
The Due Diligence refers to the steps taken to identify risks that exists within the environment. This is base on best practices, standards such as ISO 27001, ISO 17799, and other consensus. The first letter of the word Due and the word Diligence should remind you of this. The two letters are DD = Do Detect.
In the case of due care, it is the actions that you have taken (implementing, designing, enforcing, updating) to reduce the risks identified and keep them at an acceptable level. The same apply here, the first letters of the work Due and the work Care are DC. Which should remind you that DC = Do correct.
The other answers are only detractors and not valid.
Reference(s) used for this question:
CISSP Study Guide, Syngress, By Eric Conrad, Page 419
HARRIS, Shon, All-In-One CISSP Certification Exam Guide Fifth Edition, McGraw-Hill, Page 49 and 110.
and
Corporate; (Isc)² (2010-04-20). Official (ISC)2 Guide to the CISSP CBK, Second Edition ((ISC)2 Press) (Kindle Locations 11494-11504). Taylor & Francis. Kindle Edition.
and
My friend JD Murray at Techexams.net

QUESTION 348
What can best be described as a domain of trust that shares a single security policy and single management?

A. The reference monitor
B. A security domain
C. The security kernel

D. The security perimeter

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: A security domain is a domain of trust that shares a single security policy and single management.
The term security domain just builds upon the definition of domain by adding the fact that resources within this logical structure (domain) are working under the same security policy and managed by the same group.
So, a network administrator may put all of the accounting personnel, computers, and network resources in Domain 1 and all of the management personnel, computers, and network resources in Domain 2. These items fall into these individual containers because they not only carry out similar types of business functions, but also, and more importantly, have the same type of trust level. It is this common trust level that allows entities to be managed by one single security policy. The different domains are separated by logical boundaries, such as firewalls with ACLs, directory services making access decisions, and objects that have their own ACLs indicating which individuals and groups can carry out operations on them. All of these security mechanisms are examples of components that enforce the security policy for each domain. Domains can be architected in a hierarchical manner that dictates the relationship between the different domains and the ways in which subjects within the different domains can communicate. Subjects can access resources in domains of equal or lower trust levels.
The following are incorrect answers:
The reference monitor is an abstract machine which must mediate all access to subjects to objects, be protected from modification, be verifiable as correct, and is always invoked. Concept that defines a set of design requirements of a reference validation mechanism (security kernel), which enforces an access control policy over subjects' (processes, users) ability to perform operations (read, write, execute) on objects (files, resources) on a system. The reference monitor components must be small enough to test properly and be tamperproof. The security kernel is the hardware, firmware and software elements of a trusted computing base that implement the reference monitor concept.
The security perimeter includes the security kernel as well as other security-related system functions that are within the boundary of the trusted computing base. System elements that are outside of the security perimeter need not be trusted. not every process and resource falls within the TCB, so some of these components fall outside of an imaginary boundary referred to as the security perimeter. A security perimeter is a boundary that divides the trusted from the untrusted. For the system to stay in a secure and trusted state, precise communication standards must be developed to ensure that when a component within the TCB needs to communicate with a component outside the TCB, the communication cannot expose the system to unexpected security compromises. This type of communication is handled and controlled through interfaces.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 28548- 28550). McGraw-Hill. Kindle Edition.
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 7873- 7877). McGraw-Hill. Kindle Edition.
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition , Access Control, Page 214-217
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Security Architecture and Design (Kindle Locations 1280-1283). . Kindle Edition. TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation. AIO 6th edition chapter 3 access control page 214-217 defines Security domains. Reference monitor, Security Kernel, and Security Parameter are defined in Chapter 4, Security Architecture and Design.

QUESTION 349
Which of the following describes a technique in which a number of processor units are employed in a single computer system to increase the performance of the system in its application environment above the performance of a single processor of the same kind?

A. Multitasking
B. Multiprogramming
C. Pipelining
D. Multiprocessing

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Multiprocessing is an organizational technique in which a number of processor units are employed in a single computer system to increase the performance of the system in its application environment above the performance of a single processor of the same kind. In order to cooperate on a single application or class of applications, the processors share a common resource. Usually this resource is primary memory, and the multiprocessor is called a primary memory multiprocessor. A system in which each processor has a private (local) main memory and shares secondary (global) memory with the others is a secondary memory multiprocessor, sometimes called a multicomputer system because of the looser coupling between processors. The more common multiprocessor systems incorporate only processors of the same type and performance and thus are called homogeneous multiprocessors; however, heterogeneous multiprocessors are also employed. A special case is the attached processor, in which a second processor module is attached to a first processor in a closely coupled fashion so that the first can perform input/output and operating system functions, enabling the attached processor to concentrate on the application workload.
The following were incorrect answers:
Multiprogramming: The interleaved execution of two or more programs by a computer, in which the central processing unit executes a few instructions from each program in succession. Multitasking: The concurrent operation by one central processing unit of two or more processes. Pipelining: A procedure for processing instructions in a computer program more rapidly, in which each instruction is divided into numerous small stages, and a population of instructions are in various stages at any given time. One instruction does not have to wait for the previous one to complete all of the stages before it gets into the pipeline. It would be similiar to an assembly chain in the real world.

TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation. http://www.answers.com/question NO: / multiprocessing?cat=technology http://www.answers.com/multitasking?cat=biz-fin http://www.answers.com/pipelining?cat=technology

QUESTION 350
What can best be described as an abstract machine which must mediate all access to subjects to objects?

A. A security domain
B. The reference monitor
C. The security kernel
D. The security perimeter

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The reference monitor is an abstract machine which must mediate all access to subjects to objects, be protected from modification, be verifiable as correct, and is always invoked. The security kernel is the hardware, firmware and software elements of a trusted computing base that implement the reference monitor concept. The security perimeter includes the security kernel as well as other security-related system functions that are within the boundary of the trusted computing base. System elements that are outside of the security perimeter need not be trusted. A security domain is a domain of trust that shares a single security policy and single management. Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 351
Who is responsible for implementing user clearances in computer-based information systems at the B3 level of the TCSEC rating ?

A. Security administrators
B. Operators
C. Data owners

D. Data custodians

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Security administrator functions include user-oriented activities such as setting user clearances, setting initial password, setting other security characteristics for new users or changing security profiles for existing users. Data owners have the ultimate responsibility for protecting data, thus determining proper user access rights to data. Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 352
Buffer overflow and boundary condition errors are subsets of which of the following?

A. Race condition errors.
B. Access validation errors.
C. Exceptional condition handling errors.
D. Input validation errors.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: In an input validation error, the input received by a system is not properly checked, resulting in a vulnerability that can be exploited by sending a certain input sequence. There are two important types of input validation errors: buffer overflows (input received is longer than expected input length) and boundary condition error (where an input received causes the system to exceed an assumed boundary). A race condition occurs when there is a delay between the time when a system checks to see if an operation is allowed by the security model and the time when the system actually performs the operation. In an access validation error, the system is vulnerable because the access control mechanism is faulty. In an exceptional condition handling error, the system somehow becomes vulnerable due to an exceptional condition that has arisen. Source: DUPUIS, Clement, Access Control Systems and Methodology CISSP Open Study Guide, version 1.0, march 2002 (page 105).

QUESTION 353
Ensuring least privilege does not require:

A. Identifying what the user's job is.
B. Ensuring that the user alone does not have sufficient rights to subvert an important process.
C. Determining the minimum set of privileges required for a user to perform their duties.
D. Restricting the user to required privileges and nothing more.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Ensuring that the user alone does not have sufficient rights to subvert an important process is a concern of the separation of duties principle and it does not concern the least privilege principle.
Source: DUPUIS, Clément, Access Control Systems and Methodology CISSP Open Study Guide, version 1.0, march 2002 (page 33).

QUESTION 354
Who is responsible for initiating corrective measures and capabilities used when there are security violations?

A. Information systems auditor
B. Security administrator

C. Management

D. Data owners

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Management is responsible for protecting all assets that are directly or indirectly under their control.
They must ensure that employees understand their obligations to protect the company's assets, and implement security in accordance with the company policy. Finally, management is responsible for initiating corrective actions when there are security violations. Source: HARE, Chris, Security management Practices CISSP Open Study Guide, version 1.0, april 1999.

QUESTION 355
What can best be defined as high-level statements, beliefs, goals and objectives?

A. Standards

B. Policies

C. Guidelines

D. Procedures

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Policies are high-level statements, beliefs, goals and objectives and the general means for their attainment for a specific subject area. Standards are mandatory activities, action, rules or regulations designed to provide policies with the support structure and specific direction they require to be effective. Guidelines are more general statements of how to achieve the policies objectives by providing a framework within which to implement procedures. Procedures spell out the specific steps of how the policy and supporting standards and how guidelines will be implemented.
Source: HARE, Chris, Security management Practices CISSP Open Study Guide, version 1.0, april 1999.

QUESTION 356
In an organization, an Information Technology security function should:

A. Be a function within the information systems function of an organization.

B. Report directly to a specialized business unit such as legal, corporate security or insurance.

C. Be lead by a Chief Security Officer and report directly to the CEO.

D. Be independent but report to the Information Systems function.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: In order to offer more independence and get more attention from management, an IT security function should be independent from IT and report directly to the CEO. Having it report to a specialized business unit (e.g. legal) is not recommended as it promotes a low technology view of the function and leads people to believe that it is someone else's problem. Source: HARE, Chris, Security management Practices CISSP Open Study Guide, version 1.0, april 1999.

QUESTION 357
IT security measures should:

A. Be complex

B. Be tailored to meet organizational security goals.
C. Make sure that every asset of the organization is well protected.
D. Not be developed in a layered fashion.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: In general, IT security measures are tailored according to an organization's unique needs. While numerous factors, such as the overriding mission requirements, and guidance, are to be considered, the fundamental issue is the protection of the mission or business from IT securityrelated, negative impacts. Because IT security needs are not uniform, system designers and security practitioners should consider the level of trust when connecting to other external networks and internal sub-domains. Recognizing the uniqueness of each system allows a layered security strategy to be used - implementing lower assurance solutions with lower costs to protect less critical systems and higher assurance solutions only at the most critical areas. The more complex the mechanism, the more likely it may possess exploitable flaws. Simple mechanisms tend to have fewer exploitable flaws and require less maintenance. Further, because configuration management issues are simplified, updating or replacing a simple mechanism becomes a less intensive process.
Security designs should consider a layered approach to address or protect against a specific threat or to reduce a vulnerability. For example, the use of a packet-filtering router in conjunction with an application gateway and an intrusion detection system combine to increase the work-factor an attacker must expend to successfully attack the system. Adding good password controls and adequate user training improves the system's security posture even more. The need for layered protections is especially important when commercial-off-the-shelf (COTS) products are used. Practical experience has shown that the current state-of-the-art for security quality in COTS products does not provide a high degree of protection against sophisticated attacks. It is possible to help mitigate this situation by placing several controls in series, requiring additional work by attackers to accomplish their goals. Source: STONEBURNER, Gary & al, National Institute of Standards and Technology (NIST), NIST Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001 (pages 9-10).

QUESTION 358
Which of the following does not address Database Management Systems (DBMS) Security?

A. Perturbation
B. Cell suppression
C. Padded cells
D. Partitioning

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Padded cells complement Intrusion Detection Systems (IDSs) and are not related to DBMS security. Padded cells are simulated environments to which IDSs seamlessly transfer detected attackers and are designed to convince an attacker that the attack is going according to the plan. Cell suppression is a technique used against inference attacks by not revealing information in the case where a statistical query produces a very small result set. Perturbation also addresses inference attacks but involves making minor modifications to the results to a query. Partitioning involves splitting a database into two or more physical or logical parts; especially relevant for multilevel secure databases.
Source: LaROSA, Jeanette (domain leader), Application and System Development Security CISSP Open Study Guide, version 3.0, January 2002.

QUESTION 359
Which of the following security modes of operation involves the highest risk?

A. Compartmented Security Mode

B. Multilevel Security Mode
C. System-High Security Mode
D. Dedicated Security Mode

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: In multilevel mode, two or more classification levels of data exist, some people are not cleared for all the data on the system.
Risk is higher because sensitive data could be made available to someone not validated as being capable of maintaining secrecy of that data (i.e., not cleared for it). In other security modes, all users have the necessary clearance for all data on the system. Source: LaROSA, Jeanette (domain leader), Application and System Development Security CISSP Open Study Guide, version 3.0, January 2002.

QUESTION 360
During which phase of an IT system life cycle are security requirements developed?

A. Operation
B. Initiation
C. Functional design analysis and Planning
D. Implementation

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The software development life cycle (SDLC) (sometimes referred to as the System Development Life Cycle) is the process of creating or altering software systems, and the models and methodologies that people use to develop these systems. The NIST SP 800-64 revision 2 has within the description section of para 3.2.1:
This section addresses security considerations unique to the second SDLC phase. Key security activities for this phase include:
· Conduct the risk assessment and use the results to supplement the baseline security controls; · Analyze security requirements;
· Perform functional and security testing;
· Prepare initial documents for system certification and accreditation; and · Design security architecture.
Reviewing this publication you may want to pick development/acquisition. Although initiation would be a decent choice, it is correct to say during this phase you would only brainstorm the idea of security requirements. Once you start to develop and acquire hardware/software components then you would also develop the security controls for these. The Shon Harris reference below is correct as well.
Shon Harris' Book (All-in-One CISSP Certification Exam Guide) divides the SDLC differently:
Project initiation
Functional design analysis and planning
System design specifications
Software development
Installation
Maintenance support
Revision and replacement
According to the author (Shon Harris), security requirements should be developed during the functional design analysis and planning phase.
SDLC POSITIONING FROM NIST 800-64

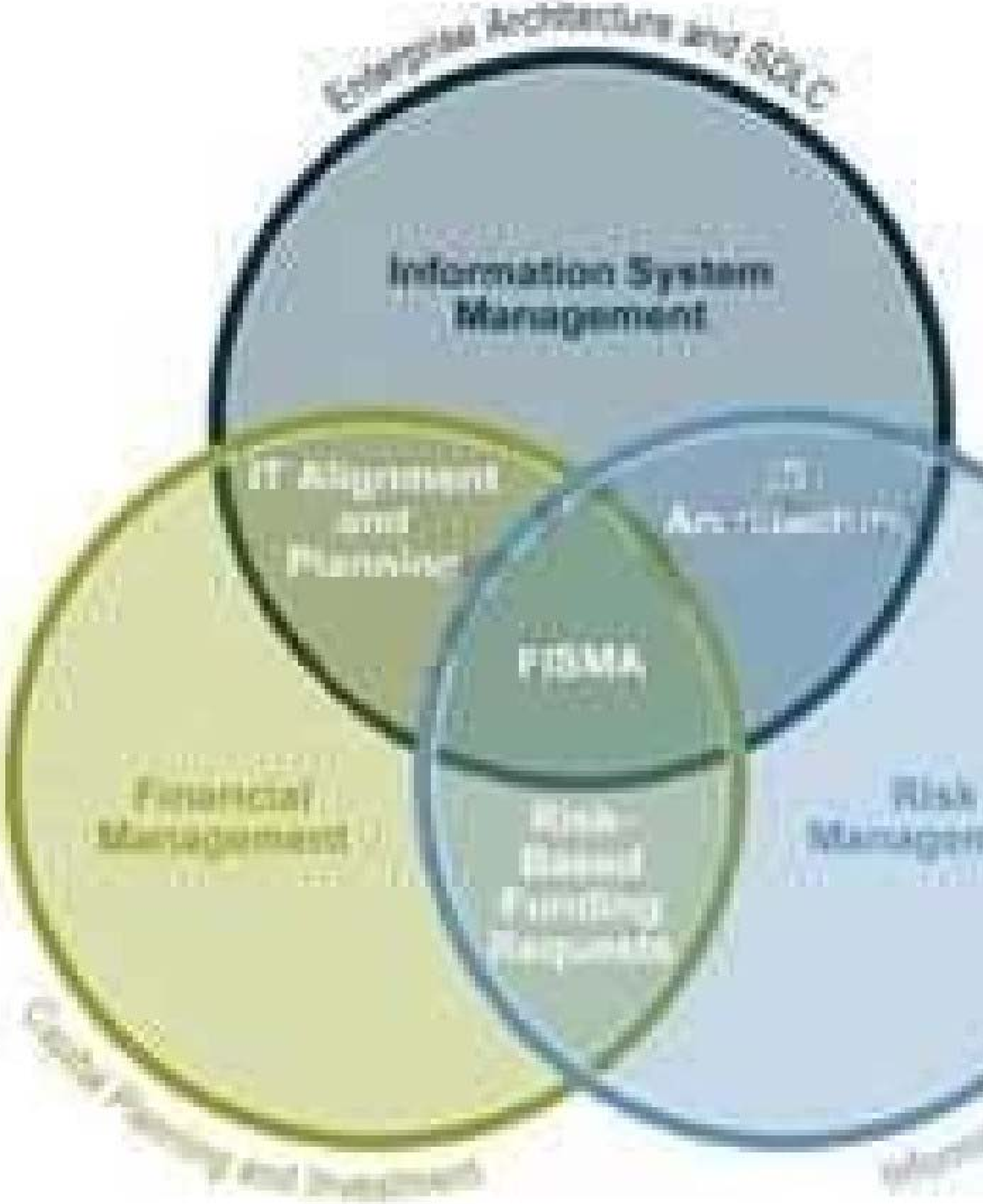

Enterprise Architecture and SDLC
Information System Management
IT Alignment and Planning
IS Architecture
FISMA
Financial Management
Risk-Based Funding Requests
Risk Managem
Capital Planning and Investment

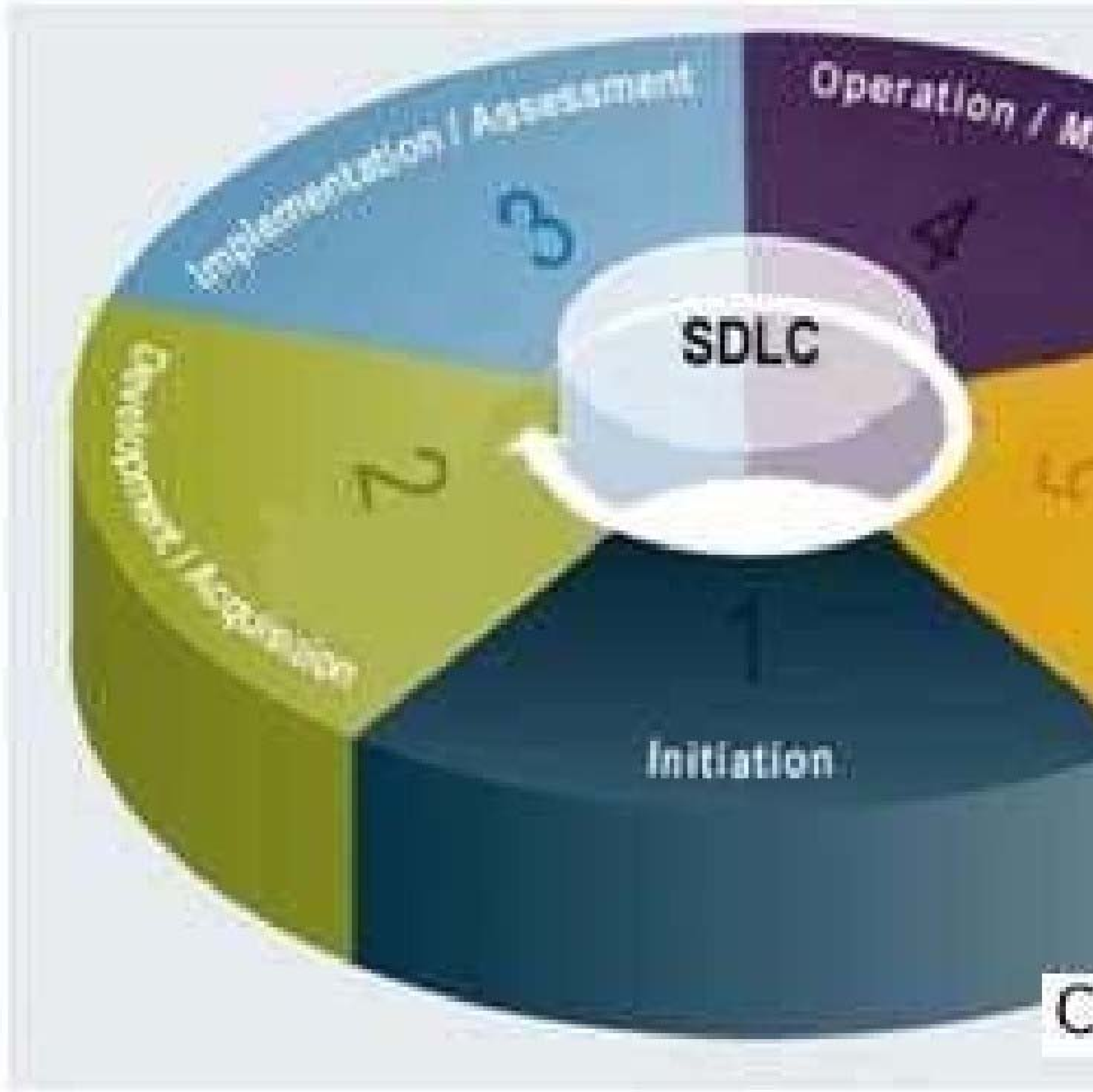
FIGURE 2-1. POSITIONING SECURIT
CONSIDERATIONS

SDLC Positioning in the enterprise

Information system security processes and activities provide valuable input into managing IT systems and their development, enabling risk identification, planning and mitigation. A risk management approach involves continually balancing the protection of agency information and assets with the cost of security controls and mitigation strategies throughout the complete information system development life cycle (see Figure 2-1 above). The most effective way to implement risk management is to identify critical assets and operations, as well as systemic vulnerabilities across the agency. Risks are shared and not bound by organization, revenue source, or topologies. Identification and verification of critical assets and operations and their interconnections can be achieved through the system security planning process, as well as through the compilation of information from the Capital Planning and Investment Control (CPIC) and Enterprise Architecture (EA) processes to establish insight into the agency's vital business operations, their supporting assets, and existing interdependencies and relationships. With critical assets and operations identified, the organization can and should perform a business impact analysis (BIA). The purpose of the BIA is to relate systems and assets with the critical services they provide and assess the consequences of their disruption. By identifying these systems, an agency can manage security effectively by establishing priorities. This positions the security office to facilitate the IT program's cost-effective performance as well as articulate its business impact and value to the agency.

SDLC OVERVIEW FROM NIST 800-64

SDLC Overview from NIST 800-64 Revision 2



NIST 800-64 Revision 2 is one publication within the NISTstandards that I would recommend you look at for more details about the SDLC. It describe in great details what activities would take place and they have a nice diagram for each of the phases of the SDLC. You will find a copy at:
http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf DISCUSSION:
Different sources present slightly different info as far as the phases names are concerned. People sometimes gets confused with some of the NIST standards. For example NIST 800-64 Security Considerations in the Information System Development Life Cycle has slightly different names, the activities mostly remains the same.
NIST clearly specifies that Security requirements would be considered throughout ALL of the phases. The

keyword here is considered, if a question is about which phase they would be developed than Functional Design Analysis would be the correct choice. Within the NIST standard they use different phase, howeverr under the second phase you will see that they talk specifically about Security Functional requirements analysis which confirms it is not at the initiation stage so it become easier to come out with the answer to this question. Here is what is stated:
The security functional requirements analysis considers the system security environment, including the enterprise information security policy and the enterprise security architecture. The analysis should address all requirements for confidentiality, integrity, and availability of information, and should include a review of all legal, functional, and other security requirements contained in applicable laws, regulations, and guidance. At the initiation step you would NOT have enough detailed yet to produce the Security Requirements. You are mostly brainstorming on all of the issues listed but you do not develop them all at that stage.
By considering security early in the information system development life cycle (SDLC), you may be able to avoid higher costs later on and develop a more secure system from the start.
NIST says:
NIST`s Information Technology Laboratory recently issued Special Publication (SP) 800-64, Security Considerations in the Information System Development Life Cycle, by Tim Grance, Joan Hash, and Marc Stevens, to help organizations include security requirements in their planning for every phase of the system life cycle, and to select, acquire, and use appropriate and cost-effective security controls.
I must admit this is all very tricky but reading skills and paying attention to KEY WORDS is a must for this exam.

HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, Fifth Edition, Page 956
and
NIST S-64 Revision 2 at http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64- Revision2.pdf
and
http://www.mks.com/resources/resource-pages/software-development-life-cycle-sdlc-system- development

QUESTION 361
Which of the following phases of a system development life-cycle is most concerned with establishing a good security policy as the foundation for design?

A. Development/acquisition
B. Implementation
C. Initiation
D. Maintenance

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: A security policy is an important document to develop while designing an information system. The security policy begins with the organization's basic commitment to information security formulated as a general policy statement. The policy is then applied to all aspects of the system design or security solution. The policy identifies security goals (e.g., confidentiality, integrity, availability, accountability, and assurance) the system should support, and these goals guide the procedures, standards and controls used in the IT security architecture design.
The policy also should require definition of critical assets, the perceived threat, and securityrelated roles and responsibilities.
Source: STONEBURNER, Gary & al, National Institute of Standards and Technology (NIST), NIST Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001 (page 6).

QUESTION 362
When considering an IT System Development Life-cycle, security should be:

A. Mostly considered during the initiation phase.
B. Mostly considered during the development phase.

C. Treated as an integral part of the overall system design.
D. Added once the design is completed.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Security must be considered in information system design. Experience has shown it is very difficult to implement security measures properly and successfully after a system has been developed, so it should be integrated fully into the system life-cycle process. This includes establishing security policies, understanding the resulting security requirements, participating in the evaluation of security products, and finally in the engineering, design, implementation, and disposal of the system.
Source: STONEBURNER, Gary & al, National Institute of Standards and Technology (NIST), NIST Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001 (page 7).

QUESTION 363
Risk reduction in a system development life-cycle should be applied:

A. Mostly to the initiation phase.
B. Mostly to the development phase.
C. Mostly to the disposal phase.
D. Equally to all phases.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Risk is defined as the combination of the probability that a particular threat source will exploit, or trigger, a particular information system vulnerability and the resulting mission impact should this occur. Previously, risk avoidance was a common IT security goal. That changed as the nature of the risk became better understood. Today, it is recognized that elimination of all risk is not cost-effective. A cost-benefit analysis should be conducted for each proposed control. In some cases, the benefits of a more secure system may not justify the direct and indirect costs. Benefits include more than just prevention of monetary loss; for example, controls may be essential for maintaining public trust and confidence. Direct costs include the cost of purchasing and installing a given technology; indirect costs include decreased system performance and additional training. The goal is to enhance mission/business capabilities by managing mission/business risk to an acceptable level.
Source: STONEBURNER, Gary & al, National Institute of Standards and Technology (NIST), NIST Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001 (page 8).

QUESTION 364
Which of the following phases of a system development life-cycle is most concerned with maintaining proper authentication of users and processes to ensure appropriate access control decisions?

A. Development/acquisition
B. Implementation
C. Operation/Maintenance
D. Initiation

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The operation phase of an IT system is concerned with user authentication. Authentication is the

process where a system establishes the validity of a transmission, message, or a means of verifying the eligibility of an individual, process, or machine to carry out a desired action, thereby ensuring that security is not compromised by an untrusted source. It is essential that adequate authentication be achieved in order to implement security policies and achieve security goals. Additionally, level of trust is always an issue when dealing with crossdomain interactions. The solution is to establish an authentication policy and apply it to crossdomain interactions as required.
Source: STONEBURNER, Gary & al, National Institute of Standards and Technology (NIST), NIST Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001 (page 15).

QUESTION 365
What can be defined as: It confirms that users' needs have been met by the supplied solution ?

A. Accreditation
B. Certification
C. Assurance
D. Acceptance

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Acceptance confirms that users' needs have been met by the supplied solution. Verification and Validation informs Acceptance by establishing the evidence set against acceptance criteria - to determine if the solution meets the users' needs. Acceptance should also explicitly address any integration or interoperability requirements involving other equipment or systems. To enable acceptance every user and system requirement must have a 'testable' characteristic.
Accreditation is the formal acceptance of security, adequacy, authorization for operation and acceptance of existing risk. Accreditation is the formal declaration by a Designated Approving Authority (DAA) that an IS is approved to operate in a particular security mode using a prescribed set of safeguards to an acceptable level of risk.
Certification is the formal testing of security safeguards and assurance is the degree of confidence that the implemented security measures work as intended. The certification is a Comprehensive evaluation of the technical and nontechnical security features of an IS and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified ecurity requirements. Assurance is the descriptions of the measures taken during development and evaluation of the product to assure compliance with the claimed security functionality. For example, an evaluation may require that all source code is kept in a change management system, or that full functional testing is performed. The Common Criteria provides a catalogue of these, and the requirements may vary from one evaluation to the next. The requirements for particular targets or types of products are documented in the Security Targets (ST) and Protection Profiles (PP), respectively. Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 4, August 1999.
and
Official ISC2 Guide to the CISSP CBK, Second Edition, on page 211.
and
http://www.aof.mod.uk/aofcontent/tactical/randa/content/randaintroduction.htm

QUESTION 366
Which of the following statements pertaining to the security kernel is incorrect?

A. The security kernel is made up of mechanisms that fall under the TCB and implements and enforces the reference monitor concept.
B. The security kernel must provide isolation for the processes carrying out the reference monitor concept and they must be tamperproof.
C. The security kernel must be small enough to be able to be tested and verified in a completeand comprehensive manner.
D. The security kernel is an access control concept, not an actual physical component.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The reference monitor, not the security kernel is an access control concept. The security kernel is made up of software, and firmware components that fall within the TCB and implements and enforces the reference monitor concept. The security kernel mediates all access and functions between subjects and objects. The security kernel is the core of the TCB and is the most commonly used approach to building trusted computing systems. There are three main requirements of the security kernel:
· It must provide isolation for the processes carrying out the reference monitor concept, and the processes must be tamperproof.
· It must be invoked for every access attempt and must be impossible to circumvent. Thus, the security kernel must be implemented in a complete and foolproof way. · It must be small enough to be able to be tested and verified in a complete and comprehensive manner.
The following answers are incorrect:
The security kernel is made up of mechanisms that fall under the TCB and implements and enforces the reference monitor concept. Is incorrect because this is the definition of the security kernel.
The security kernel must provide isolation for the processes carrying out the reference monitor concept and they must be tamperproof. Is incorrect because this is one of the three requirements that make up the security kernel.
The security kernel must be small enough to be able to be tested and verified in a complete and comprehensive manner. Is incorrect because this is one of the three requirements that make up the security kernel.

QUESTION 367
Which of the following best corresponds to the type of memory addressing where the address location that is specified in the program instruction contains the address of the final desired location?

A. Direct addressing
B. Indirect addressing
C. Indexed addressing
D. Program addressing

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Indirect addressing is when the address location that is specified in the program instruction contains the address of the final desired location. Direct addressing is when a portion of primary memory is accessed by specifying the actual address of the memory location. Indexed addressing is when the contents of the address defined in the program's instruction is added to that of an index register. Program addressing is not a defined memory addressing mode. Source: WALLHOFF, John, CBK#6 Security Architecture and Models (CISSP Study Guide), April 2002 (page 2).

QUESTION 368
Which of the following security mode of operation does NOT require all users to have the clearance for all information processed on the system?

A. Compartmented security mode
B. Multilevel security mode
C. System-high security mode
D. Dedicated security mode

Correct Answer: B
Explanation

Explanation/Reference:

Explanation: The multilevel security mode permits two or more classification levels of information to be processed at the same time when all the users do not have the clearance of formal approval to access all the information being processed by the system. In dedicated security mode, all users have the clearance or authorization and need-to-know to all data processed within the system.

In system-high security mode, all users have a security clearance or authorization to access the information but not necessarily a need-to-know for all the information processed on the system (only some of the data).

In compartmented security mode, all users have the clearance to access all the information processed by the system, but might not have the need-to-know and formal access approval. Generally, Security modes refer to information systems security modes of operations used in mandatory access control (MAC) systems. Often, these systems contain information at various levels of security classification.

The mode of operation is determined by:

The type of users who will be directly or indirectly accessing the system. The type of data, including classification levels, compartments, and categories, that are processed on the system.

The type of levels of users, their need to know, and formal access approvals that the users will have.

Dedicated security mode

In this mode of operation, all users must have:

Signed NDA for ALL information on the system.

Proper clearance for ALL information on the system.

Formal access approval for ALL information on the system. A valid need to know for ALL information on the system.

All users can access ALL data.

System high security mode

In this mode of operation, all users must have:

Signed NDA for ALL information on the system.

Proper clearance for ALL information on the system.

Formal access approval for ALL information on the system. A valid need to know for SOME information on the system. All users can access SOME data, based on their need to know.

Compartmented security mode

In this mode of operation, all users must have:

Signed NDA for ALL information on the system.

Proper clearance for ALL information on the system.

Formal access approval for SOME information they will access on the system. A valid need to know for SOME information on the system. All users can access SOME data, based on their need to know and formal access approval.

Multilevel security mode

In this mode of operation, all users must have:

Signed NDA for ALL information on the system.

Proper clearance for SOME information on the system.

Formal access approval for SOME information on the system. A valid need to know for SOME information on the system. All users can access SOME data, based on their need to know, clearance and formal access approval.

WALLHOFF, John, CBK#6 Security Architecture and Models (CISSP Study Guide), April 2002 (page 6).
and
http://en.wikipedia.org/wiki/Security_Modes

QUESTION 369

What prevents a process from accessing another process' data?

A. Memory segmentation
B. Process isolation
C. The reference monitor
D. Data hiding

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Process isolation is where each process has its own distinct address space for its application code and data. In this way, it is possible to prevent each process from accessing another process' data. This prevents data leakage, or modification to the data while it is in memory. Memory segmentation is a virtual memory management mechanism. The reference monitor is an abstract machine that mediates all accesses to objects by subjects. Data hiding, also known as information hiding, is a mechanism that makes information available at one processing level is not available at another level.
Source: HARE, Chris, Security Architecture and Models, Area 6 CISSP Open Study Guide, January 2002.

QUESTION 370
What can best be defined as the sum of protection mechanisms inside the computer, including hardware, firmware and software?

A. Trusted system
B. Security kernel
C. Trusted computing base
D. Security perimeter

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The Trusted Computing Base (TCB) is defined as the total combination of protection mechanisms within a computer system. The TCB includes hardware, software, and firmware. These are part of the TCB because the system is sure that these components will enforce the security policy and not violate it.
The security kernel is made up of hardware, software, and firmware components at fall within the TCB and implements and enforces the reference monitor concept.
AIOv4 Security Models and Architecture pgs 268, 273

QUESTION 371
A trusted system does NOT involve which of the following?

A. Enforcement of a security policy.
B. Sufficiency and effectiveness of mechanisms to be able to enforce a security policy.
C. Assurance that the security policy can be enforced in an efficient and reliable manner.
D. Independently-verifiable evidence that the security policy-enforcing mechanisms are sufficient and effective.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: A trusted system is one that meets its intended security requirements. It involves sufficiency and effectiveness, not necessarily efficiency, in enforcing a security policy. Put succinctly, trusted systems have (1) policy, (2) mechanism, and (3) assurance. Source: HARE, Chris, Security Architecture and Models, Area 6 CISSP Open Study Guide, January 2002.

QUESTION 372
What can be described as an imaginary line that separates the trusted components of the TCB from those elements that are NOT trusted?

A. The security kernel
B. The reference monitor
C. The security perimeter
D. The reference perimeter

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The security perimeter is the imaginary line that separates the trusted components of the kernel and the Trusted Computing Base (TCB) from those elements that are not trusted. The reference monitor is an abstract machine that mediates all accesses to objects by subjects. The security kernel can be software, firmware or hardware components in a trusted system and is the actual instantiation of the reference monitor. The reference perimeter is not defined and is a distracter.
Source: HARE, Chris, Security Architecture and Models, Area 6 CISSP Open Study Guide, January 2002.

QUESTION 373
A Security Kernel is defined as a strict implementation of a reference monitor mechanism responsible for enforcing a security policy. To be secure, the kernel must meet three basic conditions, what are they?

A. Confidentiality, Integrity, and Availability
B. Policy, mechanism, and assurance
C. Isolation, layering, and abstraction
D. Completeness, Isolation, and Verifiability

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: A security kernel is responsible for enforcing a security policy. It is a strict implementation of a reference monitor mechanism. The architecture of a kernel operating system is typically layered, and the kernel should be at the lowest and most primitive level. It is a small portion of the operating system through which all references to information and all changes to authorizations must pass. In theory, the kernel implements access control and information flow control between implemented objects according to the security policy. To be secure, the kernel must meet three basic conditions:
completeness (all accesses to information must go through the kernel), isolation (the kernel itself must be protected from any type of unauthorized access), and verifiability (the kernel must be proven to meet design specifications). The reference monitor, as noted previously, is an abstraction, but there may be a reference validator, which usually runs inside the security kernel and is responsible for performing security access checks on objects, manipulating privileges, and generating any resulting security audit messages.
A term associated with security kernels and the reference monitor is the trusted computing base (TCB). The TCB is the portion of a computer system that contains all elements of the system responsible for supporting the security policy and the isolation of objects. The security capabilities of products for use in the TCB can be verified through various evaluation criteria, such as the earlier Trusted Computer System Evaluation Criteria (TCSEC) and the current Common Criteria standard.
Many of these security terms--reference monitor, security kernel, TCB--are defined loosely by vendors for purposes of marketing literature. Thus, it is necessary for security professionals to read the small print and between the lines to fully understand what the vendor is offering in regard to security features.
TIP FOR THE EXAM:
The terms Security Kernel and Reference monitor are synonymous but at different levels.
As it was explained by Diego:
While the Reference monitor is the concept, the Security kernel is the implementation of such concept (via hardware, software and firmware means).
The two terms are the same thing, but on different levels: one is conceptual, one is "technical" The following are incorrect answers:
Confidentiality, Integrity, and Availability
Policy, mechanism, and assurance
Isolation, layering, and abstraction
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 13858-13875). Auerbach Publications. Kindle Edition.

QUESTION 374

What can best be defined as the detailed examination and testing of the security features of an IT system or product to ensure that they work correctly and effectively and do not show any logical vulnerabilities, such as evaluation criteria?

A. Acceptance testing

B. Evaluation

C. Certification

D. Accreditation

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Evaluation as a general term is described as the process of independently assessing a system against a standard of comparison, such as evaluation criteria. Evaluation criterias are defined as a benchmark, standard, or yardstick against which accomplishment, conformance, performance, and suitability of an individual, hardware, software, product, or plan, as well as of risk-reward ratio is measured.
What is computer security evaluation?
Computer security evaluation is the detailed examination and testing of the security features of an IT system or product to ensure that they work correctly and effectively and do not show any logical vulnerabilities. The Security Target determines the scope of the evaluation. It includes a claimed level of Assurance that determines how rigorous the evaluation is.
Criteria
Criteria are the "standards" against which security evaluation is carried out. They define several degrees of rigour for the testing and the levels of assurance that each confers. They also define the formal requirements needed for a product (or system) to meet each Assurance level.
TCSEC
The US Department of Defense published the first criteria in 1983 as the Trusted Computer Security Evaluation Criteria (TCSEC), more popularly known as the "Orange Book". The current issue is dated 1985. The US Federal Criteria were drafted in the early 1990s as a possible replacement but were never formally adopted.
ITSEC
During the 1980s, the United Kingdom, Germany, France and the Netherlands produced versions of their own national criteria. These were harmonised and published as the Information Technology Security Evaluation Criteria (ITSEC). The current issue, Version 1.2, was published by the European Commission in June 1991. In September 1993, it was followed by the IT Security Evaluation Manual (ITSEM) which specifies the methodology to be followed when carrying out ITSEC evaluations.
Common Criteria
The Common Criteria represents the outcome of international efforts to align and develop the existing European and North American criteria. The Common Criteria project harmonises ITSEC, CTCPEC (Canadian Criteria) and US Federal Criteria (FC) into the Common Criteria for Information Technology Security Evaluation (CC) for use in evaluating products and systems and for stating security requirements in a standardised way. Increasingly it is replacing national and regional criteria with a worldwide set accepted by the International Standards Organisation (ISO15408).
The following answer were not applicable:
Certification is the process of performing a comprehensive analysis of the security features and safeguards of a system to establish the extent to which the security requirements are satisfied. Shon Harris states in her book that Certification is the comprehensive technical evaluation of the security components and their compliance for the purpose of accreditation. Wikipedia describes it as: Certification is a comprehensive evaluation of the technical and nontechnical security controls (safeguards) of an information system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements
Accreditation is the official management decision to operate a system. Accreditation is the formal declaration by a senior agency official (Designated Accrediting Authority (DAA) or Principal Accrediting Authority (PAA)) that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural security controls (safeguards).
Acceptance testing refers to user testing of a system before accepting delivery.
Reference(s) used for this question:

HARE, Chris, Security Architecture and Models, Area 6 CISSP Open Study Guide, January 2002.
and
https://en.wikipedia.org/wiki/Certification_and_Accreditation and
http://www.businessdictionary.com/definition/evaluation-criteria.html and
http://www.cesg.gov.uk/products_services/iacs/cc_and_itsec/secevalcriteria.shtml

QUESTION 375
Which of the following is NOT a common integrity goal?

A. Prevent unauthorized users from making modifications.
B. Maintain internal and external consistency.
C. Prevent authorized users from making improper modifications.
D. Prevent paths that could lead to inappropriate disclosure.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Inappropriate disclosure is a confidentiality, not an integrity goal. All of the other choices above are integrity goals addressed by the Clark-Wilson integrity model. The Clark-Wilson model is an integrity model that addresses all three integrity goals:
1. prevent unauthorized users from making modifications,
2. prevent authorized users from making improper modifications, and
3. maintain internal and external consistency through auditing. NOTE: Biba address only the first goal of integrity above Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 1384). McGraw-Hill.
Kindle Edition.

QUESTION 376
When it comes to magnetic media sanitization, what difference can be made between clearing and purging information?

A. Clearing completely erases the media whereas purging only removes file headers, allowing the recovery of files.
B. Clearing renders information unrecoverable by a keyboard attack and purging renders information unrecoverable against laboratory attack.
C. They both involve rewriting the media.
D. Clearing renders information unrecoverable against a laboratory attack and purging renders information unrecoverable to a keyboard attack.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The removal of information from a storage medium is called sanitization. Different kinds of sanitization provide different levels of protection. A distinction can be made between clearing information (rendering it unrecoverable by a keyboard attack) and purging (rendering it unrecoverable against laboratory attack).
There are three general methods of purging media: overwriting, degaussing, and destruction. There should be continuous assurance that sensitive information is protected and not allowed to be placed in a circumstance wherein a possible compromise can occur. There are two primary levels of threat that the protector of information must guard against: keyboard attack (information scavenging through system software capabilities) and laboratory attack (information scavenging through laboratory means). Procedures should be implemented to address these threats before the Automated Information System (AIS) is procured, and the procedures should be continued throughout the life cycle of the AIS.
Reference(s) use for this question:
SWANSON, Marianne & GUTTMAN, Barbara, National Institute of Standards and Technology (NIST), NIST

Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996 (page 26).
and
A guide to understanding Data Remanence in Automated Information Systems

QUESTION 377
What is the main issue with media reuse?

A. Degaussing
B. Data remanence
C. Media destruction
D. Purging

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The main issue with media reuse is data remanence, where residual information still resides on a media that has been erased. Degaussing, purging and destruction are ways to handle media that contains data that is no longer needed or used. Source: WALLHOFF, John, CBK#10 Physical Security (CISSP Study Guide), April 2002 (page 5).

QUESTION 378
Which of the following should NOT be performed by an operator?

A. Implementing the initial program load
B. Monitoring execution of the system
C. Data entry
D. Controlling job flow

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Under the principle of separation of duties, an operator should not be performing data entry. This should be left to data entry personnel. System operators represent a class of users typically found in data center environments where mainframe systems are used. They provide day-to-day operations of the mainframe environment, ensuring that scheduled jobs are running effectively and troubleshooting problems that may arise. They also act as the arms and legs of the mainframe environment, load and unloading tape and results of job print runs. Operators have elevated privileges, but less than those of system administrators. If misused, these privileges may be used to circumvent the system's security policy. As such, use of these privileges should be monitored through audit logs. Some of the privileges and responsibilities assigned to operators include:
Implementing the initial program load: This is used to start the operating system. The boot process or initial program load of a system is a critical time for ensuring system security. Interruptions to this process may reduce the integrity of the system or cause the system to crash, precluding its availability.
Monitoring execution of the system: Operators respond to various events, to include errors, interruptions, and job completion messages.
Volume mounting: This allows the desired application access to the system and its data. Controlling job flow: Operators can initiate, pause, or terminate programs. This may allow an operator to affect the scheduling of jobs. Controlling job flow involves the manipulation of configuration information needed by the system. Operators with the ability to control a job or application can cause output to be altered or diverted, which can threaten the confidentiality. Bypass label processing: This allows the operator to bypass security label information to run foreign tapes (foreign tapes are those from a different data center that would not be using the same label format that the system could run). This privilege should be strictly controlled to prevent unauthorized access.
Renaming and relabeling resources: This is sometimes necessary in the mainframe environment to allow

programs to properly execute. Use of this privilege should be monitored, as it can allow the unauthorized viewing of sensitive information.
Reassignment of ports and lines: Operators are allowed to reassign ports or lines. If misused, reassignment can cause program errors, such as sending sensitive output to an unsecured location. Furthermore, an incidental port may be opened, subjecting the system to an attack through the creation of a new entry point into the system.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 19367-19395). Auerbach Publications. Kindle Edition. Which of the following should be performed by an operator?

A. Changing profiles
B. Approving changes
C. Adding and removal of users
D. Installing system software

Answer: D
Of the listed tasks, installing system software is the only task that should normally be performed by an operator in a properly segregated environment.
Source: MOSHER, Richard & ROTHKE, Ben, CISSP CBK Review presentation on domain 7.

QUESTION 379
Which of the following is not appropriate in addressing object reuse?

A. Degaussing magnetic tapes when they're no longer needed.
B. Deleting files on disk before reusing the space.
C. Clearing memory blocks before they are allocated to a program or data.
D. Clearing buffered pages, documents, or screens from the local memory of a terminal or printer.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Object reuse requirements, applying to systems rated TCSEC C2 and above, are used to protect files, memory, and other objects in a trusted system from being accidentally accessed by users who are not authorized to access them. Deleting files on disk merely erases file headers in a directory structure. It does not clear data from the disk surface, thus making files still recoverable. All other options involve clearing used space, preventing any unauthorized access. Source: RUSSEL, Deborah & GANGEMI, G.T. Sr., Computer Security Basics, O'Reilly, July 1992 (page 119).

QUESTION 380
Who of the following is responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of IT systems and data?

A. Business and functional managers
B. IT Security practitioners
C. System and information owners
D. Chief information officer

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The system and information owners are responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of the IT systems and data they own. IT security practitioners are responsible for proper implementation of security requirements in their IT systems.
Source: STONEBURNER, Gary et al., NIST Special publication 800-30, Risk management Guide for

Information Technology Systems, 2001 (page 6).

QUESTION 381
An effective information security policy should not have which of the following characteristic?

A. Include separation of duties
B. Be designed with a short- to mid-term focus
C. Be understandable and supported by all stakeholders
D. Specify areas of responsibility and authority

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: An effective information security policy should be designed with a long-term focus.
All other characteristics apply.
Source: ALLEN, Julia H., The CertKingdom to System and Network Security Practices, Addison- Wesley, 2001, Appendix B, Practice-Level Policy Considerations (page 397).

QUESTION 382
Which of the following choice is NOT normally part of the questions that would be asked in regards to an organization's information security policy?

A. Who is involved in establishing the security policy?
B. Where is the organization's security policy defined?
C. What are the actions that need to be performed in case of a disaster?
D. Who is responsible for monitoring compliance to the organization's security policy?

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Actions to be performed in case of a disaster are not normally part of an information security policy but part of a Disaster Recovery Plan (DRP). Only personnel implicated in the plan should have a copy of the Disaster Recovery Plan whereas everyone should be aware of the contents of the organization's information security policy. Source: ALLEN, Julia H., The CertKingdom to System and Network Security Practices, Addison- Wesley, 2001, Appendix B, Practice-Level Policy Considerations (page 398).

QUESTION 383
The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system is referred to as?

A. Confidentiality
B. Availability
C. Integrity
D. Reliability

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: An company security program must:
1) assure that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability;
2) protect informationcommensurate with the level of risk and magnitude ofharmresulting fromloss, misuse, unauthorized access, or modification.

The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system; i.e., a system is available if it provides services according to the system design whenever users request them.
The following are incorrect answers:
Confidentiality - The information requires protection from unauthorized disclosure and only the INTENDED recipient should have access to the meaning of the data either in storage or in transit. Integrity - The information must be protected from unauthorized, unanticipated, or unintentional modification. This includes, but is not limited to:
Authenticity A third party must be able to verify that the content of a message has not been changed in transit.
Non-repudiation The origin or the receipt of a specific message must be verifiable by a third party.
Accountability - A security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.
Reference used for this question:
RFC 2828
and
SWANSON, Marianne, NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001 (page 5).

QUESTION 384
Which of the following is most concerned with personnel security?

A. Management controls
B. Operational controls
C. Technical controls
D. Human resources controls

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Many important issues in computer security involve human users, designers, implementers, and managers.
A broad range of security issues relates to how these individuals interact with computers and the access and authorities they need to do their jobs. Since operational controls address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems), personnel security is considered a form of operational control. Operational controls are put in place to improve security of a particular system (or group of systems). They often require specialized expertise and often rely upon management activities as well as technical controls. Implementing dual control and making sure that you have more than one person that can perform a task would fall into this category as well. Management controls focus on the management of the IT security system and the management of risk for a system. They are techniques and concerns that are normally addressed by management. Technical controls focus on security controls that the computer system executes. The controls can provide automated protection for unauthorized access of misuse, facilitate detection of security violations, and support security requirements for applications and data.
Reference use for this question:
NIST SP 800-53 Revision 4 http://dx.doi.org/10.6028/NIST.SP.800-53r4 You can get it as a word document by clicking HERE
NIST SP 800-53 Revision 4 has superseded the document below:
SWANSON, Marianne, NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001 (Page A-18).

QUESTION 385
Which of the following would best classify as a management control?

A. Review of security controls
B. Personnel security
C. Physical and environmental protection
D. Documentation

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Management controls focus on the management of the IT security system and the management of risk for a system.
They are techniques and concerns that are normally addressed by management. Routine evaluations and response to identified vulnerabilities are important elements of managing the risk of a system, thus considered management controls. SECURITY CONTROLS: The management, operational, and technical controls (i.e.,safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
SECURITY CONTROL BASELINE: The set of minimum security controls defined for a low-impact, moderate-impact,or high-impact information system.
The following are incorrect answers:
Personnel security, physical and environmental protection and documentation are forms of operational controls.
Reference(s) used for this question:
http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf and
FIPS PUB 200 at http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

QUESTION 386
Which of the following is not a form of passive attack?

A. Scavenging
B. Data diddling
C. Shoulder surfing
D. Sniffing

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Data diddling involves alteration of existing data and is extremely common. It is one of the easiest types of crimes to prevent by using access and accounting controls, supervision, auditing, separation of duties, and authorization limits. It is a form of active attack. All other choices are examples of passive attacks, only affecting confidentiality. Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/ Osborne, 2002, Chapter 10: Law, Investigation, and Ethics (page 645).

QUESTION 387
Which of the following statements pertaining to a security policy is incorrect?

A. Its main purpose is to inform the users, administrators and managers of their obligatory requirements for protecting technology and information assets.
B. It specifies how hardware and software should be used throughout the organization.
C. It needs to have the acceptance and support of all levels of employees within the organization in order for it to be appropriate and effective.
D. It must be flexible to the changing environment.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: A security policy would NOT define how hardware and software should be used throughout the organization. A standard or a procedure would provide such details but not a policy.
A security policy is a formal statement of the rules that people who are given access to anorganization's technology and information assets must abide. The policy communicates the security goals to all of the users,

the administrators, and the managers. The goals will be largely determined by the following key tradeoffs: services offered versus security provided, ease of use versus security, and cost of security versus risk of loss. The main purpose of a security policy is to inform the users, the administrators and the managers of their obligatory requirements for protecting technology and information assets. The policy should specify the mechanisms through which these requirements can be met. Another purpose is to provide a baseline from which to acquire, configure and audit computer systems and networks for compliance with the policy. In order for a security policy to be appropriate and effective, it needs to have the acceptance and support of all levels of employees within the organization. A good security policy must:

· Be able to be implemented through system administration procedures, publishing of acceptable use guidelines, or other appropriate methods

· Be able to be enforced with security tools, where appropriate, and with sanctions, where actual prevention is not technically feasible

· Clearly define the areas of responsibility for the users, the administrators, and the managers · Be communicated to all once it is established

· Be flexible to the changing environment of a computer network since it is a living document Reference(s) used for this question:

National Security Agency, Systems and Network Attack Center (SNAC),The 60 Minute Network Security Guide, February 2002, page 7.

or

A local copy is kept at:

https://www.freepracticetests.org/documents/The%2060%20Minute%20Network%20Security%20 Guide.pdf

QUESTION 388

Which of the following statements pertaining to software testing is incorrect?

A. Unit testing should be addressed and considered when the modules are being designed.

B. Test data should be part of the specifications.

C. Testing should be performed with live data to cover all possible situations.

D. Test data generators can be used to systematically generate random test data that can be used to test programs.

Correct Answer: C

Explanation

Explanation/Reference:

Explanation: Live or actual field data is not recommended for use in the testing procedures because both data types may not cover out of range situations and the correct outputs of the test are unknown. Live data would not be the best data to use because of the lack of anomalies and also because of the risk of exposure to your live data. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 251).

QUESTION 389

Which of the following can be defined as the process of rerunning a portion of the test scenario or test plan to ensure that changes or corrections have not introduced new errors?

A. Unit testing

B. Pilot testing

C. Regression testing

D. Parallel testing

Correct Answer: C

Explanation

Explanation/Reference:

Explanation: Regression testing is the process of rerunning a portion of the test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be the

same as the data used in the original test. Unit testing refers to the testing of an individual program or module. Pilot testing is a preliminary test that focuses only on specific and predetermined aspects of a system. Parallel testing is the process of feeding test data into two systems and comparing the results.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 300).

QUESTION 390
Which of the following statements pertaining to software testing approaches is correct?

A. A bottom-up approach allows interface errors to be detected earlier.
B. A top-down approach allows errors in critical modules to be detected earlier.
C. The test plan and results should be retained as part of the system's permanent documentation.
D. Black box testing is predicated on a close examination of procedural detail.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: A bottom-up approach to testing begins testing of atomic units, such as programs or modules, and works upwards until a complete system testing has taken place. It allows errors in critical modules to be found early. A top-down approach allows for early detection of interface errors and raises confidence in the system, as programmers and users actually see a working system. White box testing is predicated on a close examination of procedural detail. Black box testing examines some aspect of the system with little regard for the internal logical structure of the software.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 300).
Top Down Testing: An approach to integration testing where the component at the top of the component hierarchy is tested first, with lower level components being simulated by stubs. Tested components are then used to test lower level components. The process is repeated until the lowest level components have been tested.
Bottom Up Testing: An approach to integration testing where the lowest level components are tested first, then used to facilitate the testing of higher level components. The process is repeated until the component at the top of the hierarchy is tested. Black Box Testing: Testing based on an analysis of the specification of a piece of software without reference to its internal workings. The goal is to test how well the component conforms to the published requirements for the component.

QUESTION 391
Which of the following test makes sure the modified or new system includes appropriate access controls and does not introduce any security holes that might compromise other systems?

A. Recovery testing
B. Security testing
C. Stress/volume testing
D. Interface testing

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Security testing makes sure the modified or new system includes appropriate access controls and does not introduce any security holes that might compromise other systems. Recovery testing checks the system's ability to recover after a software or hardware failure. Stress/volume testing involves testing an application with large quantities of data in order to evaluate performance during peak hours.
Interface testing evaluates the connection of two or more components that pass information from one area to another.

Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 300).

QUESTION 392
Which of the following phases of a software development life cycle normally addresses Due Care and Due Diligence?

A. Implementation
B. System feasibility
C. Product design
D. Software plans and requirements

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The software plans and requirements phase addresses threats, vulnerabilities, security requirements, reasonable care, due diligence, legal liabilities, cost/benefit analysis, level of protection desired, test plans.
Implementation is incorrect because it deals with Installing security software, running the system, acceptance testing, security software testing, and complete documentation certification and accreditation (where necessary).
System Feasibility is incorrect because it deals with information security policy, standards, legal issues, and the early validation of concepts.
Product design is incorrect because it deals with incorporating security specifications, adjusting test plans and data,
determining access controls, design documentation, evaluating encryption options, and verification.
Sources:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 252).
KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter 7: Security Life Cycle Components, Figure 7.5 (page 346).

QUESTION 393
Which of the following phases of a software development life cycle normally incorporates the security specifications, determines access controls, and evaluates encryption options?

A. Detailed design
B. Implementation
C. Product design
D. Software plans and requirements

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The Product design phase deals with incorporating security specifications, adjusting test plans and data, determining access controls, design documentation, evaluating encryption options, and verification.
Implementation is incorrect because it deals with Installing security software, running the system, acceptance testing, security software testing, and complete documentation certification and accreditation (where necessary).
Detailed design is incorrect because it deals with information security policy, standards, legal issues, and the early validation of concepts.
software plans and requirements is incorrect because it deals with addressesing threats, vulnerabilities, security requirements, reasonable care, due diligence, legal liabilities, cost/benefit analysis, level of protection desired, test plans.

Sources:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 252).
KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter 7: Security Life Cycle Components, Figure 7.5 (page 346). At which of the basic phases of the System Development Life Cycle are security requirements formalized?
A. Disposal
B. System Design Specifications
C. Development and Implementation
D. Functional Requirements Definition

Answer: D
During the Functional Requirements Definition the project management and systems development teams will conduct a comprehensive analysis of current and possible future functional requirements to ensure that the new system will meet end-user needs. The teams also review the documents from the project initiation phase and make any revisions or updates as needed. For smaller projects, this phase is often subsumed in the project initiation phase. At this point security requirements should be formalized.
The Development Life Cycle is a project management tool that can be used to plan, execute, and control a software development project usually called the Systems Development Life Cycle (SDLC).
The SDLC is a process that includes systems analysts, software engineers, programmers, and end users in the project design and development. Because there is no industry-wide SDLC, an organization can use any one, or a combination of SDLC methods. The SDLC simply provides a framework for the phases of a software development project from defining the functional requirements to implementation. Regardless of the method used, the SDLC outlines the essential phases, which can be shown together or as separate elements. The model chosen should be based on the project.
For example, some models work better with long-term, complex projects, while others are more suited for short-term projects. The key element is that a formalized SDLC is utilized. The number of phases can range from three basic phases (concept, design, and implement) on up.
The basic phases of SDLC are:
Project initiation and planning
Functional requirements definition
System design specifications
Development and implementation
Documentation and common program controls
Testing and evaluation control, (certification and accreditation) Transition to production (implementation)
The system life cycle (SLC) extends beyond the SDLC to include two additional phases:
Operations and maintenance support (post-installation) Revisions and system replacement
System Design Specifications
This phase includes all activities related to designing the system and software. In this phase, the system architecture, system outputs, and system interfaces are designed. Data input, data flow, and output requirements are established and security features are designed, generally based on the overall security architecture for the company.
Development and Implementation
During this phase, the source code is generated, test scenarios and test cases are developed, unit and integration testing is conducted, and the program and system are documented for maintenance and for turnover to acceptance testing and production. As well as general care for software quality, reliability, and consistency of operation, particular care should be taken to ensure that the code is analyzed to eliminate common vulnerabilities that might lead to security exploits and other risks.
Documentation and Common Program Controls
These are controls used when editing the data within the program, the types of logging the program should be doing, and how the program versions should be stored. A large number of such controls may be needed, see the reference below for a full list of controls.
Acceptance
In the acceptance phase, preferably an independent group develops test data and tests the code to ensure that it will function within the organization's environment and that it meets all the functional and security requirements. It is essential that an independent group test the code during all applicable stages of development to prevent a separation of duties issue. The goal of security testing is to ensure that the application meets its security requirements and specifications. The security testing should uncover all design and implementation flaws that would allow a user to violate the software security policy and requirements. To

ensure test validity, the application should be tested in an environment that simulates the production environment. This should include a security certification package and any user documentation. Certification and Accreditation (Security Authorization) Certification is the process of evaluating the security stance of the software or system against a predetermined set of security standards or policies. Certification also examines how well the system performs its intended functional requirements. The certification or evaluation document should contain an analysis of the technical and nontechnical security features and countermeasures and the extent to which the software or system meets the security requirements for its mission and operational environment.

Transition to Production (Implementation)

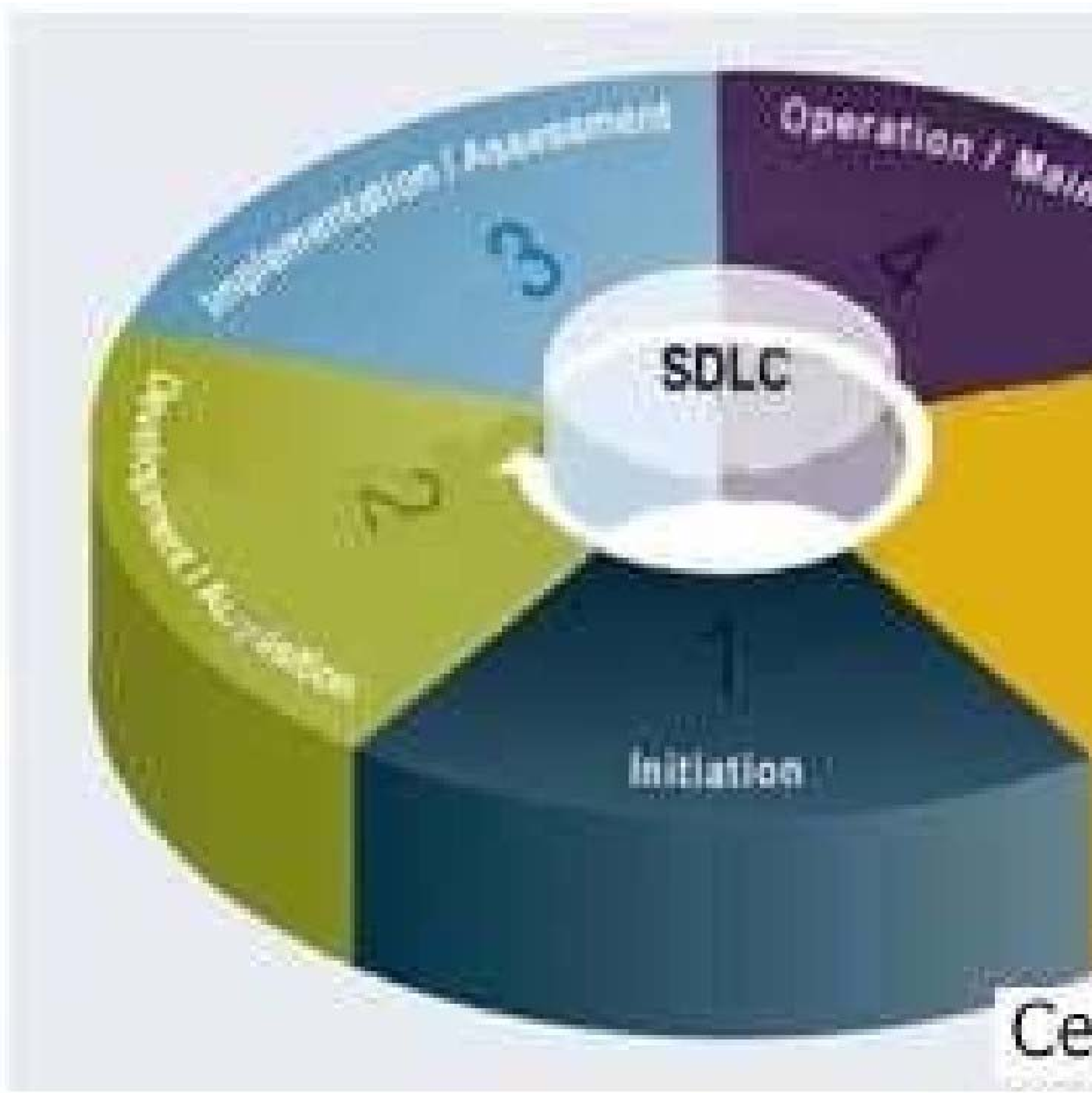
During this phase, the new system is transitioned from the acceptance phase into the live production environment. Activities during this phase include obtaining security accreditation; training the new users according to the implementation and training schedules; implementing the system, including installation and data conversions; and, if necessary, conducting any parallel operations.

Revisions and System Replacement

As systems are in production mode, the hardware and software baselines should be subject to periodic evaluations and audits. In some instances, problems with the application may not be defects or flaws, but rather additional functions not currently developed in the application. Any changes to the application must follow the same SDLC and be recorded in a change management system. Revision reviews should include security planning and procedures to avoid future problems. Periodic application audits should be conducted and include documenting security incidents when problems occur. Documenting system failures is a valuable resource for justifying future system enhancements.

Below you have the phases used by NIST in it's 800-63 Revision 2 document As noted above, the phases will vary from one document to another one. For the purpose of the exam use the list provided in the official ISC2 Study book which is presented in short form above. Refer to the book for a more detailed description of activities at each of the phases of the SDLC. However, all references have very similar steps being used. As mentioned in the official book, it could be as simple as three phases in it's most basic version (concept, design, and implement) or a lot more in more detailed versions of the SDLC.

The key thing is to make use of an SDLC.



SDLC phases
Reference(s) used for this question:
NIST SP 800-64 Revision 2 at http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64- Revision2.pdf and
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition: Software Development Security ((ISC)2 Press) (Kindle Locations 134-157). Auerbach Publications. Kindle Edition.

QUESTION 394
Which of the following is less likely to be included in the change control sub-phase of the maintenance phase

of a software product?

A. Estimating the cost of the changes requested
B. Recreating and analyzing the problem
C. Determining the interface that is presented to the user
D. Establishing the priorities of requests

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Change control sub-phase includes Recreating and analyzing the problem, Determining the interface that is presented to the user, and Establishing the priorities of requests. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 252).

QUESTION 395
What is the act of obtaining information of a higher sensitivity by combining information from lower levels of sensitivity?

A. Polyinstantiation
B. Inference
C. Aggregation
D. Data mining

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Aggregation is the act of obtaining information of a higher sensitivity by combining information from lower levels of sensitivity.
The incorrect answers are:
Polyinstantiation is the development of a detailed version of an object from another object using different values in the new object.
Inference is the ability of users to infer or deduce information about data at sensitivity levels for which they do not have access privilege.
Data mining refers to searching through a data warehouse for data correlations.
Sources:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 261).
KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter 7: Database Security Issues (page 358).

QUESTION 396
Which expert system operating mode allows determining if a given hypothesis is valid?

A. Blackboard
B. Lateral chaining
C. Forward chaining
D. Backward chaining

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Backward-chaining mode - the expert system backtracks to determine if a given hypothesis is

valid. Backward-chaining is generally used when there are a large number of possible solutions relative to the number of inputs.
Incorrect answers are:
In a forward-chaining mode, the expert system acquires information and comes to a conclusion based on that information. Forward-chaining is the reasoning approach that can be used when there is a small number of solutions relative to the number of inputs. Blackboard is an expert system-reasoning methodology in which a solution is generated by the use of a virtual blackboard, wherein information or potential solutions are placed on the blackboard by a plurality of individuals or expert knowledge sources. As more information is placed on the blackboard in an iterative process, a solution is generated.
Lateral-chaining mode - No such expert system mode.
Sources:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 259).
KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter 7: Expert Systems (page 354).

QUESTION 397
Why does compiled code pose more of a security risk than interpreted code?

A. Because malicious code can be embedded in compiled code and be difficult to detect.
B. If the executed compiled code fails, there is a chance it will fail insecurely.
C. Because compilers are not reliable.
D. There is no risk difference between interpreted code and compiled code.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: From a security standpoint, a compiled program is less desirable than an interpreted one because malicious code can be
resident somewhere in the compiled code, and it is difficult to detect in a very large program.

QUESTION 398
Which software development model is actually a meta-model that incorporates a number of the software development models?

A. The Waterfall model
B. The modified Waterfall model
C. The Spiral model
D. The Critical Path Model (CPM)

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The spiral model is actually a meta-model that incorporates a number of the software development models. This model depicts a spiral that incorporates the various phases of software development. The model states that each cycle of the spiral involves the same series of steps for each part of the project. CPM refers to the Critical Path Methodology. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 246).

QUESTION 399
Which of the following is used in database information security to hide information?

A. Inheritance

B. Polyinstantiation

C. Polymorphism

D. Delegation

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Polyinstantiation enables a relation to contain multiple tuples with the same primary keys with each instance distinguished by a security level. When this information is inserted into a database, lower-level subjects need to be restricted from this information. Instead of just restricting access, another set of data is created to fool the lower-level subjects into thinking that the information actually means something else.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 11: Application and System Development (page 727).

QUESTION 400
Which of the following computer design approaches is based on the fact that in earlier technologies, the instruction fetch was the longest part of the cycle?

A. Pipelining

B. Reduced Instruction Set Computers (RISC)

C. Complex Instruction Set Computers (CISC)

D. Scalar processors

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Complex Instruction Set Computer (CISC) uses instructions that perform many operations per instruction. It was based on the fact that in earlier technologies, the instruction fetch was the longest part of the cycle. Therefore, by packing more operations into an instruction, the number of fetches could be reduced. Pipelining involves overlapping the steps of different instructions to increase the performance in a computer. Reduced Instruction Set Computers (RISC) involve simpler instructions that require fewer clock cycles to execute. Scalar processors are processors that execute one instruction at a time. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architectures and Models (page 188).

QUESTION 401
What is used to protect programs from all unauthorized modification or executional interference?

A. A protection domain

B. A security perimeter

C. Security labels

D. Abstraction

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: A protection domain consists of the execution and memory space assigned to each process. The purpose of establishing a protection domain is to protect programs from all unauthorized modification or executional interference. The security perimeter is the boundary that separates the Trusted Computing Base (TCB) from the remainder of the system. Security labels are assigned to resources to denote a type of classification. Abstraction is a way to protect resources in the fact that it involves viewing system components at a high level and ignoring its specific details, thus performing information hiding.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of

Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architecture and Models (page 193).

QUESTION 402
What is called a system that is capable of detecting that a fault has occurred and has the ability to correct the fault or operate around it?

A. A fail safe system
B. A fail soft system
C. A fault-tolerant system
D. A failover system

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: A fault-tolerant system is capable of detecting that a fault has occurred and has the ability to correct the fault or operate around it. In a fail-safe system, program execution is terminated, and the system is protected from being compromised when a hardware or software failure occurs and is detected. In a fail-soft system, when a hardware or software failure occurs and is detected, selected, non-critical processing is terminated. The term failover refers to switching to a duplicate "hot" backup component in real-time when a hardware or software failure occurs, enabling processing to continue.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architecture and Models (page 196).

QUESTION 403
What is defined as the hardware, firmware and software elements of a trusted computing base that implement the reference monitor concept?

A. The reference monitor
B. Protection rings
C. A security kernel
D. A protection domain

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: A security kernel is defined as the hardware, firmware and software elements of a trusted computing base that implement the reference monitor concept. A reference monitor is a system component that enforces access controls on an object. A protection domain consists of the execution and memory space assigned to each process. The use of protection rings is a scheme that supports multiple protection domains.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architecture and Models (page 194).

QUESTION 404
Which of the following rules is least likely to support the concept of least privilege?

A. The number of administrative accounts should be kept to a minimum.
B. Administrators should use regular accounts when performing routine operations like reading mail.
C. Permissions on tools that are likely to be used by hackers should be as restrictive as possible.
D. Only data to and from critical systems and applications should be allowed through the firewall.

Correct Answer: D
Explanation

Explanation/Reference:

Explanation: Only data to and from critical systems and applications should be allowed through the firewall is a detractor. Critical systems or applications do not necessarily need to have traffic go through a firewall. Even if they did, only the minimum required services should be allowed. Systems that are not deemed critical may also need to have traffic go through the firewall. Least privilege is a basic tenet of computer security that means users should be given only those rights required to do their jobs or tasks. Least privilege is ensuring that you have the minimum privileges necessary to do a task. An admin NOT using his admin account to check email is a clear example of this.
Reference(s) used for this question:
National Security Agency, Systems and Network Attack Center (SNAC), The 60 Minute Network Security Guide, February 2002, page 9.

QUESTION 405
Which of the following is an unintended communication path that is NOT protected by the system's normal security mechanisms?

A. A trusted path
B. A protection domain
C. A covert channel
D. A maintenance hook

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: A covert channel is an unintended communication path within a system, therefore it is not protected by the system's normal security mechanisms. Covert channels are a secret way to convey information.
Covert channels are addressed from TCSEC level B2.
The following are incorrect answers:
A trusted path is the protected channel that allows a user to access the Trusted Computing Base (TCB) without being compromised by other processes or users. A protection domain consists of the execution and memory space assigned to each process. A maintenance hook is a hardware or software mechanism that was installed to permit system maintenance and to bypass the system's security protections.
Reference used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 6: Operations Security (page 219).

QUESTION 406
Which of the following is used to interrupt the opportunity to use or perform collusion to subvert operation for fraudulent purposes?

A. Key escrow
B. Rotation of duties
C. Principle of need-to-know
D. Principle of least privilege

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Job rotations reduce the risk of collusion of activities between individuals. Companies with individuals working with sensitive information or systems where there might be the opportunity for personal gain through collusion can benefit by integrating job rotation with segregation of duties. Rotating the position may uncover activities that the individual is performing outside of the normal operating procedures, highlighting errors or fraudulent behavior. Rotation of duties is a method of reducing the risk associated with a subject performing a (sensitive) task by limiting the amount of time the subject is assigned to perform the task before being moved to a different task.

The following are incorrect answers:
Key escrow is related to the protection of keys in storage by splitting the key in pieces that will be controlled by different departments. Key escrow is the process of ensuring a third party maintains a copy of a private key or key needed to decrypt information. Key escrow also should be considered mandatory for most organization's use of cryptography as encrypted information belongs to the organization and not the individual; however often an individual's key is used to encrypt the information.
Separation of duties is a basic control that prevents or detects errors and irregularities by assigning responsibility for different parts of critical tasks to separate individuals, thus limiting the effect a single person can have on a system. One individual should not have the capability to execute all of the steps of a particular process. This is especially important in critical business areas, where individuals may have greater access and capability to modify, delete, or add data to the system. Failure to separate duties could result in individuals embezzling money from the company without the involvement of others.
The need-to-know principle specifies that a person must not only be cleared to access classified or other sensitive information, but have requirement for such information to carry out assigned job duties. Ordinary or limited user accounts are what most users are assigned. They should be restricted only to those privileges that are strictly required, following the principle of least privilege. Access should be limited to specific objects following the principle of need-to-know. The principle of least privilege requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. Least privilege refers to granting users only the accesses that are required to perform their job functions. Some employees will require greater access than others based upon their job functions. For example, an individual performing data entry on a mainframe system may have no need for Internet access or the ability to run reports regarding the information that they are entering into the system. Conversely, a supervisor may have the need to run reports, but should not be provided the capability to change information in the database.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 10628-10631). Auerbach Publications. Kindle Edition.
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 10635-10638). Auerbach Publications. Kindle Edition.
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 10693-10697). Auerbach Publications. Kindle Edition.
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 16338-16341). Auerbach Publications. Kindle Edition.

QUESTION 407
Which of the following is best defined as an administrative declaration by a designated authority that an information system is approved to operate in a particular security configuration with a prescribed set of safeguards?

A. Certification
B. Declaration
C. Audit
D. Accreditation

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Accreditation: is an administrative declaration by a designated authority that an information system is approved to operate in a particular security configuration with a prescribed set of safeguards. It is usually based on a technical certification of the system's security mechanisms.
Certification: Technical evaluation (usually made in support of an accreditation action) of an information system \'s security features and other safeguards to establish the extent to which the system\'s design and implementation meet specified security requirements. Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 408
Which of the following is best defined as a circumstance in which a collection of information items is required to be classified at a higher security level than any of the individual items that comprise it?

A. Aggregation
B. Inference
C. Clustering
D. Collision

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The Internet Security Glossary (RFC2828) defines aggregation as a circumstance in which a collection of information items is required to be classified at a higher security level than any of the individual items that comprise it.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 409
Which of the following best defines add-on security?

A. Physical security complementing logical security measures.
B. Protection mechanisms implemented as an integral part of an information system.
C. Layer security.
D. Protection mechanisms implemented after an information system has become operational.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The Internet Security Glossary (RFC2828) defines add-on security as "The retrofitting of protection mechanisms, implemented by hardware or software, after the [automatic data processing] system has become operational."
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 410
Which of the following is best defined as a mode of system termination that automatically leaves system processes and components in a secure state when a failure occurs or is detected in a system?

A. Fail proof
B. Fail soft
C. Fail safe
D. Fail Over

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: NOTE: This question is referring to a system which is Logical/Technical, so it is in the context of a system that you must choose the right answer. This is very important to read the question carefully and to identify the context whether it is in the Physical world or in the Technical/Logical world.
RFC 2828 (Internet Security Glossary) defines fail safe as a mode of system termination that automatically leaves system processes and components in a secure state when a failure occurs or is detected in the system.
A secure state means in the Logical/Technical world that no access would be granted or no packets would be allowed to flow through the system inspecting the packets such as a firewall for example.
If the question would have made reference to a building or something specific to the Physical world then the

answer would have been different. In the Physical World everything becomes open and full access would be granted. See the valid choices below for the Physical context. Fail-safe in the physical security world is when doors are unlocked automatically in case of emergency. Used in environment where humans work around. As human safety is prime concern during Fire or other hazards.

The following were all wrong choices:

Fail-secure in the physical security world is when doors are locked automatically in case of emergency. Can be in an area like Cash Locker Room provided there should be alternative manually operated exit door in case of emergency.

Fail soft is selective termination of affected non-essential system functions and processes when a failure occurs or is detected in the system.

Fail Over is a redundancy mechanism and does not apply to this question. There is a great post within the CCCure Forums on this specific question NO: :

saintrockz who is a long term contributor to the forums did outstanding research and you have the results below. The CCCure forum is a gold mine where thousands of question NO: s related to the CBK have been discussed.

According to the Official ISC2 Study Guide (OIG):

Fault Tolerance is defined as built-in capability of a system to provide continued correct execution in the presence of a limited number of hardware or software faults. It means a system can operate in the presence of hardware component failures. A single component failure in a fault-tolerant system will not cause a system interruption because the alternate component will take over the task transparently. As the cost of components continues to drop, and the demand for system availability increases, many non-fault-tolerant systems have redundancy built-in at the subsystem level. As a result, many non-fault-tolerant systems can tolerate hardware faults - consequently, the line between a fault-tolerant system and a non-fault-tolerant system becomes increasingly blurred.

According to Common Criteria:

Fail Secure - Failure with preservation of secure state, which requires that the TSF (TOE security functions) preserve a secure state in the face of the identified failures.

Acc. to The CISSP Prep Guide, Gold Ed.:

Fail over - When one system/application fails, operations will automatically switch to the backup system.

Fail safe - Pertaining to the automatic protection of programs and/or processing systems to maintain safety when a hardware or software failure is detected in a system. Fail secure - The system preserves a secure state during and after identified failures occur. Fail soft - Pertaining to the selective termination of affected non-essential processing when a hardware or software failure is detected in a system.

Acc. to CISSP for Dummies:

Fail closed - A control failure that results all accesses blocked. Fail open - A control failure that results in all accesses permitted. Failover - A failure mode where, if a hardware or software failure is detected, the system automatically transfers processing to a hot backup component, such as a clustered server. Fail-safe - A failure mode where, if a hardware or software failure is detected, program execution is terminated, and the system is protected from compromise. Fail-soft (or resilient) - A failure mode where, if a hardware or software failure is detected, certain, noncritical processing is terminated, and the computer or network continues to function in a degraded mode.

Fault-tolerant - A system that continues to operate following failure of a computer or network component.

It's good to differentiate this concept in Physical Security as well:

Fail-safe

· Door defaults to being unlocked

· Dictated by fire codes

Fail-secure

· Door defaults to being locked

Reference(s) used for this question:

SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 411

The preliminary steps to security planning include all of the following EXCEPT which of the following?

A. Establish objectives.

B. List planning assumptions.

C. Establish a security audit function.

D. Determine alternate courses of action

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The keyword within the question is: preliminary This means that you are starting your effort, you cannot audit if your infrastructure is not even in place.
Reference used for this question:
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 412
Step-by-step instructions used to satisfy control requirements is called a:

A. policy
B. standard
C. guideline
D. procedure

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 413
One purpose of a security awareness program is to modify:

A. employee's attitudes and behaviors towards enterprise's security posture
B. management's approach towards enterprise's security posture
C. attitudes of employees with sensitive data
D. corporate attitudes about safeguarding data

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The
Answer: security awareness training is to modify employees behaviour and attitude towards towards enterprise's security posture. Security-awareness training is performed to modify employees' behavior and attitude toward security. This can best be achieved through a formalized process of security-awareness training. It is used to increase the overall awareness of security throughout the company. It is targeted to every single employee and not only to one group of users. Unfortunately you cannot apply a patch to a human being, the only thing you can do is to educate employees and make them more aware of security issues and threats. Never underestimate human stupidity.
Reference(s) used for this question:
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.
also see:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 130). McGraw-Hill.
Kindle Edition.

QUESTION 414
Whose role is it to assign classification level to information?

A. Security Administrator
B. User
C. Owner

D. Auditor

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The Data/Information Owner is ultimately responsible for the protection of the data. It is the Data/ Information Owner that decides upon the classifications of that data they are responsible for.
The data owner decides upon the classification of the data he is responsible for and alters that classification if the business need arises.
The following answers are incorrect:
Security Administrator. Is incorrect because this individual is responsible for ensuring that the access right granted are correct and support the polices and directives that the Data/Information Owner defines.
User. Is Incorrect because the user uses/access the data according to how the Data/Information Owner defined their access.
Auditor. Is incorrect because the Auditor is responsible for ensuring that the access levels are appropriate. The Auditor would verify that the Owner classified the data properly.
CISSP All In One Third Edition, Shon Harris, Page 121

QUESTION 415
Which of the following security controls might force an operator into collusion with personnel assigned organizationally within a different function in order to gain access to unauthorized data?

A. Limiting the local access of operations personnel
B. Job rotation of operations personnel
C. Management monitoring of audit logs
D. Enforcing regular password changes

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The questions specifically said: "within a different function" which eliminate Job Rotation as a choice.
Management monitoring of audit logs is a detective control and it would not prevent collusion. Changing passwords regularly would not prevent such attack. This question validates if you understand the concept of separation of duties and least privilege. By having operators that have only the minimum access level they need and only what they need to do their duties within a company, the operations personnel would be force to use collusion to defeat those security mechanism.
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 416
What is the most secure way to dispose of information on a CD-ROM?

A. Sanitizing
B. Physical damage
C. Degaussing
D. Physical destruction

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: First you have to realize that the question is specifically talking about a CDROM. The information stored on a CDROM is not in electro magnetic format, so a degausser woud be inneffective.
You cannot sanitize a CDROM but you might be able to sanitize a RW/CDROM. A CDROM is a write once device and cannot be overwritten like a hard disk or other magnetic device. Physical Damage would not be

enough as information could still be extracted in a lab from the undamaged portion of the media or even from the pieces after the physical damage has been done.
Physical Destruction using a shredder, your microwave oven, melting it, would be very effective and the best choice for a non magnetic media such as a CDROM. Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 417
The Reference Validation Mechanism that ensures the authorized access relationships between subjects and objects is implementing which of the following concept:

A. The reference monitor.
B. Discretionary Access Control.
C. The Security Kernel.
D. Mandatory Access Control.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The reference monitor concept is an abstract machine that ensures that all subjects have the necessary access rights before accessing objects. Therefore, the kernel will mediates all accesses to objects by subjects and will do so by validating through the reference monitor concept.
The kernel does not decide whether or not the access will be granted, it will be the Reference Monitor which is a subset of the kernel that will say YES or NO. All access requests will be intercepted by the Kernel, validated through the reference monitor, and then access will either be denied or granted according to the request and the subject privileges within the system.
1. The reference monitor must be small enough to be full tested and valided
2. The Kernel must MEDIATE all access request from subjects to objects
3. The processes implementing the reference monitor must be protected
4. The reference monitor must be tamperproof
The following answers are incorrect:
The security kernel is the mechanism that actually enforces the rules of the reference monitor concept.
The other answers are distractors.
Shon Harris, All In One, 5th Edition, Security Architecture and Design, Page 330 also see
http://en.wikipedia.org/wiki/Reference_monitor

QUESTION 418
Which of the following describes a logical form of separation used by secure computing systems?

A. Processes use different levels of security for input and output devices.
B. Processes are constrained so that each cannot access objects outside its permitted domain.
C. Processes conceal data and computations to inhibit access by outside processes.
D. Processes are granted access based on granularity of controlled objects.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 419
What security problem is most likely to exist if an operating system permits objects to be used sequentially by multiple users without forcing a refresh of the objects?

A. Disclosure of residual data.
B. Unauthorized obtaining of a privileged execution state.

C. Denial of service through a deadly embrace.
D. Data leakage through covert channels.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: This question is asking you to consider the effects of object reuse. Object reuse is "reassigning to subject media that previously contained information. Object reuse is a security concern because if insufficient measures were taken to erase the information on the media, the information may be disclosed to unauthorized personnel." This concept relates to Security Architecture and Design, because it is in level C2: Controlled Access Protection, of the Orange Book, where "The object reuse concept must be invoked, meaning that any medium holding data must not contain any remnants of information after it is release for another subject to use."
REFERENCE:
AIO Version 5 (Shon Harris), page 360
and
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 420
At what stage of the applications development process should the security department become involved?

A. Prior to the implementation
B. Prior to systems testing
C. During unit testing
D. During requirements development

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 421
In what way could Java applets pose a security threat?

A. Their transport can interrupt the secure distribution of World Wide Web pages over the Internet by removing SSL and S-HTTP
B. Java interpreters do not provide the ability to limit system access that an applet could have on a client system.
C. Executables from the Internet may attempt an intentional attack when they are downloaded on a client system.
D. Java does not check the bytecode at runtime or provide other safety mechanisms for program isolation from the client system.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 422
Which of the following is needed for System Accountability?

A. Audit mechanisms.
B. Documented design as laid out in the Common Criteria.

C. Authorization.

D. Formal verification of system design.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Is a means of being able to track user actions. Through the use of audit logs and other tools the user actions are recorded and can be used at a later date to verify what actions were performed.
Accountability is the ability to identify users and to be able to track user actions.
The following answers are incorrect:
Documented design as laid out in the Common Criteria. Is incorrect because the Common Criteria is an international standard to evaluate trust and would not be a factor in System Accountability. Authorization. Is incorrect because Authorization is granting access to subjects, just because you have authorization does not hold the subject accountable for their actions. Formal verification of system design. Is incorrect because all you have done is to verify the system design and have not taken any steps toward system accountability.

OIG CBK Glossary (page 778)

QUESTION 423
A timely review of system access audit records would be an example of which of the basic security functions?

A. avoidance

B. deterrence

C. prevention

D. detection

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: By reviewing system logs you can detect events that have occured.
The following answers are incorrect:
avoidance. This is incorrect, avoidance is a distractor. By reviewing system logs you have not avoided anything.
deterrence. This is incorrect because system logs are a history of past events. You cannot deter something that has already occurred.
prevention. This is incorrect because system logs are a history of past events. You cannot prevent something that has already occurred.

QUESTION 424
Which of the following would assist the most in Host Based intrusion detection?

A. audit trails.

B. access control lists.

C. security clearances

D. host-based authentication

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: To assist in Intrusion Detection you would review audit logs for access violations.
The following answers are incorrect:
access control lists. This is incorrect because access control lists determine who has access to what but do not detect intrusions.

security clearances. This is incorrect because security clearances determine who has access to what but do not detect intrusions.
host-based authentication. This is incorrect because host-based authentication determine who have been authenticated to the system but do not dectect intrusions.

QUESTION 425
Who should measure the effectiveness of Information System security related controls in an organization?

A. The local security specialist
B. The business manager
C. The systems auditor
D. The central security manager

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: It is the systems auditor that should lead the effort to ensure that the security controls are in place and effective. The audit would verify that the controls comply with polices, procedures, laws, and regulations where applicable. The findings would provide these to senior management.
The following answers are incorrect:
the local security specialist. Is incorrect because an independent review should take place by a third party. The security specialist might offer mitigation strategies but it is the auditor that would ensure the effectiveness of the controls
the business manager. Is incorrect because the business manager would be responsible that the controls are in place, but it is the auditor that would ensure the effectiveness of the controls. the central security manager. Is incorrect because the central security manager would be responsible for implementing the controls, but it is the auditor that is responsibe for ensuring their effectiveness.

QUESTION 426
In an online transaction processing system (OLTP), which of the following actions should be taken when erroneous or invalid transactions are detected?

A. The transactions should be dropped from processing.
B. The transactions should be processed after the program makes adjustments.
C. The transactions should be written to a report and reviewed.
D. The transactions should be corrected and reprocessed.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: In an online transaction processing system (OLTP) all transactions are recorded as they occur. When erroneous or invalid transactions are detected the transaction can be recovered by reviewing the logs.
As explained in the ISC2 OIG:
OLTP is designed to record all of the business transactions of an organization as they occur. It is a data processing system facilitating and managing transaction-oriented applications. These are characterized as a system used by many concurrent users who are actively adding and modifying data to effectively change real-time data.
OLTP environments are frequently found in the finance, telecommunications, insurance, retail, transportation, and travel industries. For example, airline ticket agents enter data in the database in real-time by creating and modifying travel reservations, and these are increasingly joined by users directly making their own reservations and purchasing tickets through airline company Web sites as well as discount travel Web site portals. Therefore, millions of people may be accessing the same flight database every day, and dozens of people may be looking at a specific flight at the same time.
The security concerns for OLTP systems are concurrency and atomicity. Concurrency controls ensure that two users cannot simultaneously change the same data, or that one user cannot make changes before another

user is finished with it. In an airline ticket system, it is critical for an agent processing a reservation to complete the transaction, especially if it is the last seat available on the plane.

Atomicity ensures that all of the steps involved in the transaction complete successfully. If one step should fail, then the other steps should not be able to complete. Again, in an airline ticketing system, if the agent does not enter a name into the name data field correctly, the transaction should not be able to complete.

OLTP systems should act as a monitoring system and detect when individual processes abort, automatically restart an aborted process, back out of a transaction if necessary, allow distribution of multiple copies of application servers across machines, and perform dynamic load balancing. A security feature uses transaction logs to record information on a transaction before it is processed, and then mark it as processed after it is done. If the system fails during the transaction, the transaction can be recovered by reviewing the transaction logs. Checkpoint restart is the process of using the transaction logs to restart the machine by running through the log to the last checkpoint or good transaction. All transactions following the last checkpoint are applied before allowing users to access the data again.

Wikipedia has nice coverage on what is OLTP:

Online transaction processing, or OLTP, refers to a class of systems that facilitate and manage transaction-oriented applications, typically for data entry and retrieval transaction processing. The term is somewhat ambiguous; some understand a "transaction" in the context of computer or database transactions, while others (such as the Transaction Processing Performance Council) define it in terms of business or commercial transactions. OLTP has also been used to refer to processing in which the system responds immediately to user requests. An automatic teller machine (ATM) for a bank is an example of a commercial transaction processing application.

The technology is used in a number of industries, including banking, airlines, mailorder, supermarkets, and manufacturing. Applications include electronic banking, order processing, employee time clock systems, e-commerce, and eTrading. There are two security concerns for OLTP system: Concurrency and Atomicity

ATOMICITY

In database systems, atomicity (or atomicness) is one of the ACID transaction properties. In an atomic transaction, a series of database operations either all occur, or nothing occurs. A guarantee of atomicity prevents updates to the database occurring only partially, which can cause greater problems than rejecting the whole series outright. The etymology of the phrase originates in the Classical Greek concept of a fundamental and indivisible component; see atom.

An example of atomicity is ordering an airline ticket where two actions are required: payment, and a seat reservation. The potential passenger must either:

both pay for and reserve a seat; OR

neither pay for nor reserve a seat.

The booking system does not consider it acceptable for a customer to pay for a ticket without securing the seat, nor to reserve the seat without payment succeeding.

CONCURRENCY

Database concurrency controls ensure that transactions occur in an ordered fashion. The main job of these controls is to protect transactions issued by different users/applications from the effects of each other. They must preserve the four characteristics of database transactions ACID test: Atomicity, Consistency, Isolation, and Durability. Read http://en.wikipedia.org/wiki/ACID for more details on the ACID test.

Thus concurrency control is an essential element for correctness in any system where two database transactions or more, executed with time overlap, can access the same data, e.g., virtually in any general-purpose database system. A well established concurrency control theory exists for database systems: serializability theory, which allows to effectively design and analyze concurrency control methods and mechanisms.

Concurrency is not an issue in itself, it is the lack of proper concurrency controls that makes it a serious issue.

The following answers are incorrect:

The transactions should be dropped from processing. Is incorrect because the transactions are processed and when erroneous or invalid transactions are detected the transaction can be recovered by reviewing the logs.

The transactions should be processed after the program makes adjustments. Is incorrect because the transactions are processed and when erroneous or invalid transactions are detected the transaction can be recovered by reviewing the logs.

The transactions should be corrected and reprocessed. Is incorrect because the transactions are processed and when erroneous or invalid transactions are detected the transaction can be recovered by reviewing the logs.

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 12749-12768). Auerbach Publications. Kindle Edition.

and
http://en.wikipedia.org/wiki/Online_transaction_processing and
http://databases.about.com/od/administration/g/concurrency.htm

QUESTION 427
Who can best decide what are the adequate technical security controls in a computer-based application system in regards to the protection of the data being used, the criticality of the data, and it's sensitivity level ?

A. System Auditor
B. Data or Information Owner
C. System Manager
D. Data or Information user

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The data or information owner also referred to as "Data Owner" would be the best person. That is the individual or officer who is ultimately responsible for the protection of the information and can therefore decide what are the adequate security controls according to the data sensitivity and data criticality. The auditor would be the best person to determine the adequacy of controls and whether or not they are working as expected by the owner. The function of the auditor is to come around periodically and make sure you are doing what you are supposed to be doing. They ensure the correct controls are in place and are being maintained securely. The goal of the auditor is to make sure the organization complies with its own policies and the applicable laws and regulations.
Organizations can have internal auditors and/ or external auditors. The external auditors commonly work on behalf of a regulatory body to make sure compliance is being met. For example CobiT, which is a model that most information security auditors follow when evaluating a security program. While many security professionals fear and dread auditors, they can be valuable tools in ensuring the overall security of the organization. Their goal is to find the things you have missed and help you understand how to fix the problem.
The Official ISC2 Guide (OIG) says:
IT auditors determine whether users, owners, custodians, systems, and networks are in compliance with the security policies, procedures, standards, baselines, designs, architectures, management direction, and other requirements placed on systems. The auditors provide independent assurance to the management on the appropriateness of the security controls. The auditor examines the information systems and determines whether they are designed, configured, implemented, operated, and managed in a way ensuring that the organizational objectives are being achieved. The auditors provide top company management with an independent view of the controls and their effectiveness.
Bob is the head of payroll. He is therefore the individual with primary responsibility over the payroll database, and is therefore the information/data owner of the payroll database. In Bob's department, he has Sally and Richard working for him. Sally is responsible for making changes to the payroll database, for example if someone is hired or gets a raise. Richard is only responsible for printing paychecks. Given those roles, Sally requires both read and write access to the payroll database, but Richard requires only read access to it. Bob communicates these requirements to the system administrators (the "information/data custodians") and they set the file permissions for Sally's and Richard's user accounts so that Sally has read/write access, while Richard has only read access.
So in short Bob will determine what controls are required, what is the sensitivily and criticality of the Data. Bob will communicate this to the custodians who will implement the requirements on the systems/DB. The auditor would assess if the controls are in fact providing the level of security the Data Owner expects within the systems/DB. The auditor does not determine the sensitivity of the data or the crititicality of the data.
The other answers are not correct because:
A "system auditor" is never responsible for anything but auditing... not actually making control decisions but the auditor would be the best person to determine the adequacy of controls and then make recommendations.
A "system manager" is really just another name for a system administrator, which is actually an information custodian as explained above.
A "Data or information user" is responsible for implementing security controls on a day-to-day basis as they utilize the information, but not for determining what the controls should be or if they are adequate.

Official ISC2 Guide to the CISSP CBK, Third Edition , Page 477 Schneiter, Andrew (2013-04-15). Official (ISC) 2 Guide to the CISSP CBK, Third Edition :
Information Security Governance and Risk Management ((ISC)2 Press) (Kindle Locations 294- 298). Auerbach Publications. Kindle Edition.
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 3108- 3114).
Information Security Glossary
Responsibility for use of information resources

QUESTION 428
Attributable data should be:

A. always traced to individuals responsible for observing and recording the data
B. sometimes traced to individuals responsible for observing and recording the data
C. never traced to individuals responsible for observing and recording the data
D. often traced to individuals responsible for observing and recording the data

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: As per FDA data should be attributable, original, accurate, contemporaneous and legible. In an automated system attributability could be achieved by a computer system designed to identify individuals responsible for any input.
Source: U.S. Department of Health and Human Services, Food and Drug Administration, Guidance for Industry - Computerized Systems Used in Clinical Trials, April 1999, page 1.

QUESTION 429
Which of the following best describes signature-based detection?

A. Compare source code, looking for events or sets of events that could cause damage to a system or network.
B. Compare system activity for the behaviour patterns of new attacks.
C. Compare system activity, looking for events or sets of events that match a predefined pattern of events that describe a known attack.
D. Compare network nodes looking for objects or sets of objects that match a predefined pattern of objects that may describe a known attack.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Misuse detectors compare system activity, looking for events or sets of events that match a predefined pattern of events that describe a known attack. As the patterns corresponding to known attacks are called signatures, misuse detection is sometimes called "signature-based detection."
The most common form of misuse detection used in commercial products specifies each pattern of events corresponding to an attack as a separate signature. However, there are more sophisticated approaches to doing misuse detection (called "state-based" analysis techniques) that can leverage a single signature to detect groups of attacks.
Old Document:
BACE, Rebecca & MELL, Peter, NIST Special Publication 800-31 on Intrusion Detection Systems, Page 16.
The publication above has been replaced by 800-94 on page 2-4 The Updated URL is: http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

QUESTION 430
Which of the following is used to monitor network traffic or to monitor host audit logs in real time to determine violations of system security policy that have taken place?

A. Intrusion Detection System
B. Compliance Validation System
C. Intrusion Management System (IMS)
D. Compliance Monitoring System

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: An Intrusion Detection System (IDS) is a system that is used to monitor network traffic or to monitor host audit logs in order to determine if any violations of an organization's system security policy have taken place.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 48.

QUESTION 431
Which of the following monitors network traffic in real time?

A. network-based IDS
B. host-based IDS
C. application-based IDS
D. firewall-based IDS

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: This type of IDS is called a network-based IDS because monitors network traffic in real time.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 48.

QUESTION 432
A host-based IDS is resident on which of the following?

A. On each of the critical hosts
B. decentralized hosts
C. central hosts
D. bastion hosts

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: A host-based IDS is resident on a host and reviews the system and event logs in order to detect an attack on the host and to determine if the attack was successful. All critical serves should have a Host Based Intrusion Detection System (HIDS) installed. As you are well aware, network based IDS cannot make sense or detect pattern of attacks within encrypted traffic. A HIDS might be able to detect such attack after the traffic has been decrypted on the host. This is why critical servers should have both NIDS and HIDS.
FROM WIKIPEDIA:
A HIDS will monitor all or part of the dynamic behavior and of the state of a computer system. Much as a NIDS will dynamically inspect network packets, a HIDS might detect which program accesses what resources and assure that (say) a word-processor hasn\'t suddenly and inexplicably started modifying the system password-database. Similarly a HIDS might look at the state of a system, its stored information, whether in RAM, in the file-system, or elsewhere; and check that the contents of these appear as expected.
One can think of a HIDS as an agent that monitors whether anything/anyone - internal or external - has circumvented the security policy that the operating system tries to enforce. http://en.wikipedia.org/wiki/Host-

based_intrusion_detection_system

QUESTION 433
Which of the following usually provides reliable, real-time information without consuming network or host resources?

A. network-based IDS
B. host-based IDS
C. application-based IDS
D. firewall-based IDS

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: A network-based IDS usually provides reliable, real-time information without consuming network or host resources.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 48.

QUESTION 434
The fact that a network-based IDS reviews packets payload and headers enable which of the following?

A. Detection of denial of service
B. Detection of all viruses
C. Detection of data corruption
D. Detection of all password guessing attacks

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Because a network-based IDS reviews packets and headers, denial of service attacks can also be detected.
This question is an easy question if you go through the process of elimination. When you see an answer containing the keyword: ALL It is something a give away that it is not the proper answer. On the real exam you may encounter a few question where the use of the work ALL renders the choice invalid. Pay close attention to such keyword.
The following are incorrect answers:
Even though most IDSs can detect some viruses and some password guessing attacks, they cannot detect ALL viruses or ALL password guessing attacks. Therefore these two answers are only detractors.
Unless the IDS knows the valid values for a certain dataset, it can NOT detect data corruption.
Reference used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 48.

QUESTION 435
Which of the following reviews system and event logs to detect attacks on the host and determine if the attack was successful?

A. host-based IDS
B. firewall-based IDS
C. bastion-based IDS
D. server-based IDS

Correct Answer: A

Explanation

Explanation/Reference:
Explanation: A host-based IDS can review the system and event logs in order to detect an attack on the host and to determine if the attack was successful. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 48.

QUESTION 436
What would be considered the biggest drawback of Host-based Intrusion Detection systems (HIDS)?

A. It can be very invasive to the host operating system

B. Monitors all processes and activities on the host system only

C. Virtually eliminates limits associated with encryption

D. They have an increased level of visibility and control compared to NIDS

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The biggest drawback of HIDS, and the reason many organizations resist its use, is that it can be very invasive to the host operating system. HIDS must have the capability to monitor all processes and activities on the host system and this can sometimes interfere with normal system processing.
HIDS versus NIDS
A host-based IDS (HIDS) can be installed on individual workstations and/ or servers to watch for inappropriate or anomalous activity. HIDSs are usually used to make sure users do not delete system files, reconfigure important settings, or put the system at risk in any other way. So, whereas the NIDS understands and monitors the network traffic, a HIDS's universe is limited to the computer itself. A HIDS does not understand or review network traffic, and a NIDS does not "look in" and monitor a system's activity. Each has its own job and stays out of the other's way.
The ISC2 official study book defines an IDS as:
An intrusion detection system (IDS) is a technology that alerts organizations to adverse or unwanted activity. An IDS can be implemented as part of a network device, such as a router, switch, or firewall, or it can be a dedicated IDS device monitoring traffic as it traverses the network. When used in this way, it is referred to as a network IDS, or NIDS. IDS can also be used on individual host systems to monitor and report on file, disk, and process activity on that host. When used in this way it is referred to as a host-based IDS, or HIDS. An IDS is informative by nature and provides real-time information when suspicious activities are identified. It is primarily a detective device and, acting in this traditional role, is not used to directly prevent the suspected attack.
What about IPS?
In contrast, an intrusion prevention system (IPS), is a technology that monitors activity like an IDS but will automatically take proactive preventative action if it detects unacceptable activity. An IPS permits a predetermined set of functions and actions to occur on a network or system; anything that is not permitted is considered unwanted activity and blocked. IPS is engineered specifically to respond in real time to an event at the system or network layer. By proactively enforcing policy, IPS can thwart not only attackers, but also authorized users attempting to perform an action that is not within policy. Fundamentally, IPS is considered an access control and policy enforcement technology, whereas IDS is considered network monitoring and audit technology.
The following answers were incorrect:
All of the other answer were advantages and not drawback of using HIDS TIP FOR THE EXAM:
Be familiar with the differences that exists between an HIDS, NIDS, and IPS. Know that IDS's are mostly detective but IPS are preventive. IPS's are considered an access control and policy enforcement technology, whereas IDS's are considered network monitoring and audit technology.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 5817- 5822). McGraw-Hill. Kindle Edition.
and
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Access Control ((ISC) 2 Press), Domain1, Page 180-188 or on the kindle version look for Kindle Locations 3199-3203. Auerbach Publications.

QUESTION 437
Attributes that characterize an attack are stored for reference using which of the following Intrusion Detection System (IDS) ?

A. signature-based IDS
B. statistical anomaly-based IDS
C. event-based IDS
D. inferent-based IDS

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 49.

QUESTION 438
Which of the following is an issue with signature-based intrusion detection systems?

A. Only previously identified attack signatures are detected.
B. Signature databases must be augmented with inferential elements.
C. It runs only on the windows operating system
D. Hackers can circumvent signature evaluations.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: An issue with signature-based ID is that only attack signatures that are stored in their database are detected.
New attacks without a signature would not be reported. They do require constant updates in order to maintain their effectiveness.
Reference used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 49.

QUESTION 439
Which of the following is an IDS that acquires data and defines a "normal" usage profile for the network or host?

A. Statistical Anomaly-Based ID
B. Signature-Based ID
C. dynamical anomaly-based ID
D. inferential anomaly-based ID

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Statistical Anomaly-Based ID - With this method, an IDS acquires data and defines a "normal" usage profile for the network or host that is being monitored. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 49.

QUESTION 440

Which of the following is a disadvantage of a statistical anomaly-based intrusion detection system?

A. it may truly detect a non-attack event that had caused a momentary anomaly in the system.
B. it may falsely detect a non-attack event that had caused a momentary anomaly in the system.
C. it may correctly detect a non-attack event that had caused a momentary anomaly in the system.
D. it may loosely detect a non-attack event that had caused a momentary anomaly in the system.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Some disadvantages of a statistical anomaly-based ID are that it will not detect an attack that does not significantly change the system operating characteristics, or it may falsely detect a non-attack event that had caused a momentary anomaly in the system. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 49.

QUESTION 441
In the process of gathering evidence from a computer attack, a system administrator took a series of actions which are listed below. Can you identify which one of these actions has compromised the whole evidence collection process?

A. Using a write blocker
B. Made a full-disk image
C. Created a message digest for log files
D. Displayed the contents of a folder

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Displaying the directory contents of a folder can alter the last access time on each listed file.
Using a write blocker is wrong because using a write blocker ensure that you cannot modify the data on the host and it prevent the host from writing to its hard drives. Made a full-disk image is wrong because making a full-disk image can preserve all data on a hard disk, including deleted files and file fragments.
Created a message digest for log files is wrong because creating a message digest for log files. A message digest is a cryptographic checksum that can demonstrate that the integrity of a file has not been compromised (e.g. changes to the content of a log file) Domain: LEGAL, REGULATIONS, COMPLIANCE AND INVESTIGATIONS

AIO 3rd Edition, page 783-784
NIST 800-61 Computer Security Incident Handling guide page 3-18 to 3-20

QUESTION 442
As a result of a risk assessment, your security manager has determined that your organization needs to implement an intrusion detection system that can detect unknown attacks and can watch for unusual traffic behavior, such as a new service appearing on the network. What type of intrusion detection system would you select?

A. Protocol anomaly based
B. Pattern matching
C. Stateful matching
D. Traffic anomaly-based

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Traffic anomaly-based is the correct choice. An anomaly based IDS can detect unknown attacks. A traffic anomaly based IDS identifies any unacceptable deviation from expected behavior based on network traffic.
Protocol anomaly based is not the best choice as while a protocol anomaly based IDS can identify unknown attacks, this type of system is more suited to identifying deviations from established protocol standards such as HTTP. This type of IDS faces problems in analyzing complex or custom protocols.
Pattern matching is not the best choice as a pattern matching IDS cannot identify unknown attacks. This type of system can only compare packets against signatures of known attacks. Stateful matching is not the best choice as a statful matching IDS cannot identify unknown attacks. This type of system works by scanning traffic streams for patterns or signatures of attacks.
Official guide to the CISSP CBK. pages 198 to 201

QUESTION 443
Which of the following is NOT a characteristic of a host-based intrusion detection system?

A. A HIDS does not consume large amounts of system resources
B. A HIDS can analyse system logs, processes and resources
C. A HIDS looks for unauthorized changes to the system
D. A HIDS can notify system administrators when unusual events are identified

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: A HIDS does not consume large amounts of system resources is the correct choice. HIDS can consume inordinate amounts of CPU and system resources in order to function effectively, especially during an event.
All the other answers are characteristics of HIDSes
A HIDS can:
scrutinize event logs, critical system files, and other auditable system resources; look for unauthorized change or suspicious patterns of behavior or activity can send alerts when unusual events are discovered
Official guide to the CISSP CBK. Pages 197 to 198.

QUESTION 444
Which of the following is NOT a fundamental component of an alarm in an intrusion detection system?

A. Communications
B. Enunciator
C. Sensor
D. Response

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Response is the correct choice. A response would essentially be the action that is taken once an alarm has been produced by an IDS, but is not a fundamental component of the alarm.
The following are incorrect answers:
Communications is the component of an alarm that delivers alerts through a variety of channels such as email, pagers, instant messages and so on.
An Enunciator is the component of an alarm that uses business logic to compose the content and format of an alert and determine the recipients of that alert. A sensor is a fundamental component of IDS alarms. A sensor detects an event and produces an appropriate notification.
Domain: Access Control
Official guide to the CISSP CBK. page 203.

QUESTION 445
Which one of the following statements about the advantages and disadvantages of network-based Intrusion detection systems is true

A. Network-based IDSs are not vulnerable to attacks.
B. Network-based IDSs are well suited for modern switch-based networks.
C. Most network-based IDSs can automatically indicate whether or not an attack was successful.
D. The deployment of network-based IDSs has little impact upon an existing network.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Network-based IDSs are usually passive devices that listen on a network wire without interfering with the normal operation of a network. Thus, it is usually easy to retrofit a network to include network-based IDSs with minimal effort. Network-based IDSs are not vulnerable to attacks is not true, even thou network-based IDSs can be made very secure against attack and even made invisible to many attackers they still have to read the packets and sometimes a well crafted packet might exploit or kill your capture engine. Network-based IDSs are well suited for modern switch-based networks is not true as most switches do not provide universal monitoring ports and this limits the monitoring range of a network-based IDS sensor to a single host. Even when switches provide such monitoring ports, often the single port cannot mirror all traffic traversing the switch. Most network-based IDSs can automatically indicate whether or not an attack was successful is not true as most network-based IDSs cannot tell whether or not an attack was successful; they can only discern that an attack was initiated. This means that after a network-based IDS detects an attack, administrators must manually investigate each attacked host to determine whether it was indeed penetrated.
NIST special publication 800-31 Intrusion Detection System pages 15-16 Official guide to the CISSP CBK. Pages 196 to 197

QUESTION 446
Which protocol is NOT implemented in the Network layer of the OSI Protocol Stack?

A. hyper text transport protocol
B. Open Shortest Path First
C. Internet Protocol
D. Routing Information Protocol

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Open Shortest Path First, Internet Protocol, and Routing Information Protocol are all protocols implemented in the Network Layer.
Domain: Telecommunications and Network Security
AIO 3rd edition. Page 429
Official Guide to the CISSP CBK. Page 411

QUESTION 447
The session layer provides a logical persistent connection between peer hosts. Which of the following is one of the modes used in the session layer to establish this connection?

A. Full duplex
B. Synchronous
C. Asynchronous
D. Half simplex

Correct Answer: A

Explanation

Explanation/Reference:
Explanation: Layer 5 of the OSI model is the Session Layer. This layer provides a logical persistent connection between peer hosts. A session is analogous to a conversation that is necessary for applications to exchange information.
The session layer is responsible for establishing, managing, and closing end-to-end connections, called sessions, between applications located at different network endpoints. Dialogue control management provided by the session layer includes full-duplex, half-duplex, and simplex communications. Session layer management also helps to ensure that multiple streams of data stay synchronized with each other, as in the case of multimedia applications like video conferencing, and assists with the prevention of application related data errors. The session layer is responsible for creating, maintaining, and tearing down the session.
Three modes are offered:
(Full) Duplex: Both hosts can exchange information simultaneously, independent of each other. Half Duplex: Hosts can exchange information, but only one host at a time. Simplex: Only one host can send information to its peer. Information travels in one direction only. Another aspect of performance that is worthy of some attention is the mode of operation of the network or connection. Obviously, whenever we connect together device A and device B, there must be some way for A to send to B and B to send to
A. Many people don't realize, however, that
networking technologies can differ in terms of how these two directions of communication are handled. Depending on how the network is set up, and the characteristics of the technologies used, performance may be improved through the selection of performance-enhancing modes.
Basic Communication Modes of Operation
Let's begin with a look at the three basic modes of operation that can exist for any network connection, communications channel, or interface.
Simplex Operation
In simplex operation, a network cable or communications channel can only send information in one direction; it's a "one-way street". This may seem counter-intuitive: what's the point of communications that only travel in one direction? In fact, there are at least two different places where simplex operation is encountered in modern networking. The first is when two distinct channels are used for communication: one transmits from A to B and the other from B to
A. This is surprisingly common, even though not always obvious. For example, most if not all fiber optic communication is simplex, using one strand to send data in each direction. But this may not be obvious if the pair of fiber strands are combined into one cable. Simplex operation is also used in special types of technologies, especially ones that are asymmetric. For example, one type of satellite Internet access sends data over the satellite only for downloads, while a regular dial-up modem is used for upload to the service provider. In this case, both the satellite link and the dial-up connection are operating in a simplex mode.
Half-Duplex Operation
Technologies that employ half-duplex operation are capable of sending information in both directions between two nodes, but only one direction or the other can be utilized at a time. This is a fairly common mode of operation when there is only a single network medium (cable, radio frequency and so forth) between devices. While this term is often used to describe the behavior of a pair of devices, it can more generally refer to any number of connected devices that take turns transmitting. For example, in conventional Ethernet networks, any device can transmit, but only one may do so at a time. For this reason, regular (unswitched) Ethernet networks are often said to be "half-duplex", even though it may seem strange to describe a LAN that way.
Full-Duplex Operation
In full-duplex operation, a connection between two devices is capable of sending data in both directions simultaneously. Full-duplex channels can be constructed either as a pair of simplex links (as described above) or using one channel designed to permit bidirectional simultaneous transmissions. A full-duplex link can only connect two devices, so many such links are required if multiple devices are to be connected together.
Note that the term "full-duplex" is somewhat redundant; "duplex" would suffice, but everyone still says "full-duplex" (likely, to differentiate this mode from half-duplex). For a listing of protocols associated with Layer 5 of the OSI model, see below:
ADSP - AppleTalk Data Stream Protocol
ASP - AppleTalk Session Protocol
H.245 - Call Control Protocol for Multimedia Communication ISO-SP
OSI session-layer protocol (X.225, ISO 8327)
iSNS - Internet Storage Name Service
The following are incorrect answers:

Synchronous and Asynchronous are not session layer modes. Half simplex does not exist. By definition, simplex means that information travels one way only, so half-simplex is a oxymoron.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 5603-5636). Auerbach Publications. Kindle Edition.
and
http://www.tcpipguide.com/free/t_SimplexFullDuplexandHalfDuplexOperation.htm and
http://www.wisegeek.com/what-is-a-session-layer.htm

QUESTION 448
Which of the following tools is NOT likely to be used by a hacker?

A. Nessus
B. Saint
C. Tripwire
D. Nmap

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: It is a data integrity assurance software aimed at detecting and reporting accidental or malicious changes to data.
The following answers are incorrect :
Nessus is incorrect as it is a vulnerability scanner used by hackers in discovering vulnerabilities in a system. Saint is also incorrect as it is also a network vulnerability scanner likely to be used by hackers. Nmap is also incorrect as it is a port scanner for network exploration and likely to be used by hackers.
Reference :
Tripwire : http://www.tripwire.com
Nessus : http://www.nessus.org
Saint : http://www.saintcorporation.com/saint
Nmap : http://insecure.org/nmap

QUESTION 449
Which of the following would be LESS likely to prevent an employee from reporting an incident?

A. They are afraid of being pulled into something they don't want to be involved with.
B. The process of reporting incidents is centralized.
C. They are afraid of being accused of something they didn't do.
D. They are unaware of the company's security policies and procedures.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The reporting process should be centralized else employees won't bother.
The other answers are incorrect because :
They are afraid of being pulled into something they don't want to be involved with is incorrect as most of the employees fear of this and this would prevent them to report an incident. They are afraid of being accused of something they didn't do is also incorrect as this also prevents them to report an incident.
They are unaware of the company's security policies and procedures is also incorrect as mentioned above.
Reference : Shon Harris AIO v3 , Ch-10 : Laws , Investigatio & Ethics , Page : 675.

QUESTION 450
Which of the following would NOT violate the Due Diligence concept?

A. Security policy being outdated

B. Data owners not laying out the foundation of data protection

C. Network administrator not taking mandatory two-week vacation as planned

D. Latest security patches for servers being installed as per the Patch Management process

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: To be effective a patch management program must be in place (due diligence) and detailed procedures would specify how and when the patches are applied properly (Due Care). Remember, the question asked for NOT a violation of Due Diligence, in this case, applying patches demonstrates due care and the patch management process in place demonstrates due diligence.
Due diligence is the act of investigating and understanding the risks the company faces. A company practices by developing and implementing security policies, procedures, and standards. Detecting risks would be based on standards such as ISO 2700, Best Practices, and other published standards such as NIST standards for example. Due Diligence is understanding the current threats and risks. Due diligence is practiced by activities that make sure that the protection mechanisms are continually maintained and operational where risks are constantly being evaluated and reviewed. The security policy being outdated would be an example of violating the due diligence concept. Due Care is implementing countermeasures to provide protection from those threats. Due care is when the necessary steps to help protect the company and its resources from possible risks that have been identifed. If the information owner does not lay out the foundation of data protection (doing something about it) and ensure that the directives are being enforced (actually being done and kept at an acceptable level), this would violate the due care concept. If a company does not practice due care and due diligence pertaining to the security of its assets, it can be legally charged with negligence and held accountable for any ramifications of that negligence. Liability is usually established based on Due Diligence and Due Care or the lack of either.
A good way to remember this is using the first letter of both words within Due Diligence (DD) and Due Care (DC).
Due Diligence = Due Detect
Steps you take to identify risks based on best practices and standards.
Due Care = Due Correct.
Action you take to bring the risk level down to an acceptable level and maintaining that level over time.
The Following answer were wrong:
Security policy being outdated:
While having and enforcing a security policy is the right thing to do (due care), if it is outdated, you are not doing it the right way (due diligence). This questions violates due diligence and not due care.
Data owners not laying out the foundation for data protection:
Data owners are not recognizing the "right thing" to do. They don't have a security policy. Network administrator not taking mandatory two week vacation:
The two week vacation is the "right thing" to do, but not taking the vacation violates due diligence (not doing the right thing the right way)
Reference(s) used for this question
Shon Harris, CISSP All In One, Version 5, Chapter 3, pg 110

QUESTION 451
What is the primary goal of setting up a honeypot?

A. To lure hackers into attacking unused systems

B. To entrap and track down possible hackers

C. To set up a sacrificial lamb on the network

D. To know when certain types of attacks are in progress and to learn about attack techniques so the network can be fortified.

Correct Answer: D
Explanation

Explanation/Reference:

Explanation: The primary purpose of a honeypot is to study the attack methods of an attacker for the purposes of understanding their methods and improving defenses. "To lure hackers into attacking unused systems" is incorrect. Honeypots can serve as decoys but their primary purpose is to study the behaviors of attackers. "To entrap and track down possible hackers" is incorrect. There are a host of legal issues around enticement vs entrapment but a good general rule is that entrapment is generally prohibited and evidence gathered in a scenario that could be considered as "entrapping" an attacker would not be admissible in a court of law.
"To set up a sacrificial lamb on the network" is incorrect. While a honeypot is a sort of sacrificial lamb and may attract attacks that might have been directed against production systems, its real purpose is to study the methods of attackers with the goals of better understanding and improving network defenses.
References
AIO3, p. 213

QUESTION 452
Who is responsible for providing reports to the senior management on the effectiveness of the security controls?

A. Information systems security professionals

B. Data owners

C. Data custodians

D. Information systems auditors

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: IT auditors determine whether systems are in compliance with the security policies, procedures, standards, baselines, designs, architectures, management direction and other requirements" and "provide top company management with an independent view of the controls that have been designed and their effectiveness."
"Information systems security professionals" is incorrect. Security professionals develop the security policies and supporting baselines, etc.
"Data owners" is incorrect. Data owners have overall responsibility for information assets and assign the appropriate classification for the asset as well as ensure that the asset is protected with the proper controls.
"Data custodians" is incorrect. Data custodians care for an information asset on behalf of the data owner.

CBK, pp. 38 - 42.
AIO3. pp. 99 - 104

QUESTION 453
Which of the following are the two MOST common implementations of Intrusion Detection Systems?

A. Server-based and Host-based.

B. Network-based and Guest-based.

C. Network-based and Client-based.

D. Network-based and Host-based.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The two most common implementations of Intrusion Detection are Network-based and Host-based.
IDS can be implemented as a network device, such as a router, switch, firewall, or dedicated device monitoring traffic, typically referred to as network IDS (NIDS). The" (IDS) "technology can also be incorporated into a host system (HIDS) to monitor a single system for undesirable activities. "
A network intrusion detection system (NIDS) is a network device .... that monitors traffic traversing the network segment for which it is integrated." Remember that NIDS are usually passive in nature.

HIDS is the implementation of IDS capabilities at the host level. Its most significant difference from NIDS is that related processes are limited to the boundaries of a single-host system. However, this presents advantages in effectively detecting objectionable activities because the IDS process is running directly on the host system, not just observing it from the network.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 3649-3652). Auerbach Publications. Kindle Edition.

QUESTION 454
Network-based Intrusion Detection systems:

A. Commonly reside on a discrete network segment and monitor the traffic on that network segment.
B. Commonly will not reside on a discrete network segment and monitor the traffic on that network segment.
C. Commonly reside on a discrete network segment and does not monitor the traffic on that network segment.
D. Commonly reside on a host and and monitor the traffic on that specific host.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Network-based ID systems:
- Commonly reside on a discrete network segment and monitor the traffic on that network segment
- Usually consist of a network appliance with a Network Interface Card (NIC) that is operating in promiscuous mode and is intercepting and analyzing the network packets in real time "A passive NIDS takes advantage of promiscuous mode access to the network, allowing it to gain visibility into every packet traversing the network segment. This allows the system to inspect packets and monitor sessions without impacting the network, performance, or the systems and applications utilizing the network."
NOTE FROM CLEMENT:
A discrete network is a synonym for a SINGLE network. Usually the sensor will monitor a single network segment, however there are IDS today that allow you to monitor multiple LAN's at the same time.
References used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 62.
and
Official (ISC)2 Guide to the CISSP CBK, Hal Tipton and Kevin Henry, Page 196 and
Additional information on IDS systems can be found here:
http://en.wikipedia.org/wiki/Intrusion_detection_system

QUESTION 455
Which of the following are additional terms used to describe knowledge-based IDS and behaviorbased IDS?

A. signature-based IDS and statistical anomaly-based IDS, respectively
B. signature-based IDS and dynamic anomaly-based IDS, respectively
C. anomaly-based IDS and statistical-based IDS, respectively
D. signature-based IDS and motion anomaly-based IDS, respectively.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The two current conceptual approaches to Intrusion Detection methodology are knowledge-based ID systems and behavior-based ID systems, sometimes referred to as signature-based ID and statistical anomaly-based ID, respectively. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 63.

QUESTION 456
Which of the following Intrusion Detection Systems (IDS) uses a database of attacks, known system

vulnerabilities, monitoring current attempts to exploit those vulnerabilities, and then triggers an alarm if an attempt is found?

A. Knowledge-Based ID System
B. Application-Based ID System
C. Host-Based ID System
D. Network-Based ID System

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Knowledge-based Intrusion Detection Systems use a database of previous attacks and known system vulnerabilities to look for current attempts to exploit their vulnerabilities, and trigger an alarm if an attempt is found.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87. Application-Based ID System - "a subset of HIDS that analyze what's going on in an application using the transaction log files of the application." Source: Official ISC2 CISSP CBK Review Seminar Student Manual Version 7.0 p. 87
Host-Based ID System - "an implementation of IDS capabilities at the host level. Its most significant difference from NIDS is intrusion detection analysis, and related processes are limited to the boundaries of the host." Source: Official ISC2 Guide to the CISSP CBK - p. 197 Network-Based ID System - "a network device, or dedicated system attached to teh network, that monitors traffic traversing teh network segment for which it is integrated." Source: Official ISC2 Guide to the CISSP CBK - p. 196

QUESTION 457
Knowledge-based Intrusion Detection Systems (IDS) are more common than:

A. Network-based IDS
B. Host-based IDS
C. Behavior-based IDS
D. Application-Based IDS

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Knowledge-based IDS are more common than behavior-based ID systems. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 63. Application-Based IDS - "a subset of HIDS that analyze what's going on in an application using the transaction log files of the application." Source: Official ISC2 CISSP CBK Review Seminar Student Manual Version 7.0 p. 87
Host-Based IDS - "an implementation of IDS capabilities at the host level. Its most significant difference from NIDS is intrusion detection analysis, and related processes are limited to the boundaries of the host." Source: Official ISC2 Guide to the CISSP CBK - p. 197 Network-Based IDS - "a network device, or dedicated system attached to the network, that monitors traffic traversing the network segment for which it is integrated." Source: Official ISC2 Guide to the CISSP CBK - p. 196
CISSP for dummies a book that we recommend for a quick overview of the 10 domains has nice and concise coverage of the subject:
Intrusion detection is defined as real-time monitoring and analysis of network activity and data for potential vulnerabilities and attacks in progress. One major limitation of current intrusion detection system (IDS) technologies is the requirement to filter false alarms lest the operator (system or security administrator) be overwhelmed with data. IDSes are classified in many different ways, including active and passive, network-based and host-based, and knowledge-based and behaviorbased:
Active and passive IDS
An active IDS (now more commonly known as an intrusion prevention system -- IPS) is a system that's configured to automatically block suspected attacks in progress without any intervention required by an

operator. IPS has the advantage of providing real-time corrective action in response to an attack but has many disadvantages as well. An IPS must be placed in-line along a network boundary; thus, the IPS itself is susceptible to attack. Also, if false alarms and legitimate traffic haven't been properly identified and filtered, authorized users and applications may be improperly denied access. Finally, the IPS itself may be used to effect a Denial of Service (DoS) attack by intentionally flooding the system with alarms that cause it to block connections until no connections or bandwidth are available.

A passive IDS is a system that's configured only to monitor and analyze network traffic activity and alert an operator to potential vulnerabilities and attacks. It isn't capable of performing any protective or corrective functions on its own. The major advantages of passive IDSes are that these systems can be easily and rapidly deployed and are not normally susceptible to attack themselves.

Network-based and host-based IDS

A network-based IDS usually consists of a network appliance (or sensor) with a Network Interface Card (NIC) operating in promiscuous mode and a separate management interface. The IDS is placed along a network segment or boundary and monitors all traffic on that segment. A host-based IDS requires small programs (or agents) to be installed on individual systems to be monitored. The agents monitor the operating system and write data to log files and/or trigger alarms. A host-based IDS can only monitor the individual host systems on which the agents are installed; it doesn't monitor the entire network.

Knowledge-based and behavior-based IDS

A knowledge-based (or signature-based) IDS references a database of previous attack profiles and known system vulnerabilities to identify active intrusion attempts. Knowledge-based IDS is currently more common than behavior-based IDS.

Advantages of knowledge-based systems include the following:

It has lower false alarm rates than behavior-based IDS. Alarms are more standardized and more easily understood than behavior-based IDS. Disadvantages of knowledge-based systems include these:

Signature database must be continually updated and maintained. New, unique, or original attacks may not be detected or may be improperly classified. A behavior-based (or statistical anomalybased) IDS references a baseline or learned pattern of normal system activity to identify active intrusion attempts. Deviations from this baseline or pattern cause an alarm to be triggered.

Advantages of behavior-based systems include that they Dynamically adapt to new, unique, or original attacks. Are less dependent on identifying specific operating system vulnerabilities.

Disadvantages of behavior-based systems include

Higher false alarm rates than knowledge-based IDSes.

Usage patterns that may change often and may not be static enough to implement an effective behavior-based IDS.

QUESTION 458

Which of the following types of Intrusion Detection Systems uses behavioral characteristics of a system's operation or network traffic to draw conclusions on whether the traffic represents a risk to the network or host?

A. Network-based ID systems.

B. Anomaly Detection.

C. Host-based ID systems.

D. Signature Analysis.

Correct Answer: B

Explanation

Explanation/Reference:

Explanation: There are two basic IDS analysis methods: pattern matching (also called signature analysis) and anomaly detection.

Anomaly detection uses behavioral characteristics of a system's operation or network traffic to draw conclusions on whether the traffic represents a risk to the network or host. Anomalies may include but are not limited to:

Multiple failed log-on attempts

Users logging in at strange hours

Unexplained changes to system clocks

Unusual error messages

The following are incorrect answers:

Network-based ID Systems (NIDS) are usually incorporated into the network in a passive architecture, taking advantage of promiscuous mode access to the network. This means that it has visibility into every packet traversing the network segment. This allows the system to inspect packets and monitor sessions without impacting the network or the systems and applications utilizing the network.

Host-based ID Systems (HIDS) is the implementation of IDS capabilities at the host level. Its most significant difference from NIDS is that related processes are limited to the boundaries of a singlehost system. However, this presents advantages in effectively detecting objectionable activities because the IDS process is running directly on the host system, not just observing it from the network. This offers unfettered access to system logs, processes, system information, and device information, and virtually eliminates limits associated with encryption. The level of integration represented by HIDS increases the level of visibility and control at the disposal of the HIDS application.

Signature Analysis Some of the first IDS products used signature analysis as their detection method and simply looked for known characteristics of an attack (such as specific packet sequences or text in the data stream) to produce an alert if that pattern was detected. For example, an attacker manipulating an FTP server may use a tool that sends a specially constructed packet. If that particular packet pattern is known, it can be represented in the form of a signature that IDS can then compare to incoming packets. Pattern-based IDS will have a database of hundreds, if not thousands, of signatures that are compared to traffic streams. As new attack signatures are produced, the system is updated, much like antivirus solutions. There are drawbacks to pattern-based IDS. Most importantly, signatures can only exist for known attacks. If a new or different attack vector is used, it will not match a known signature and, thus, slip past the IDS. Additionally, if an attacker knows that the IDS is present, he or she can alter his or her methods to avoid detection. Changing packets and data streams, even slightly, from known signatures can cause an IDS to miss the attack. As with some antivirus systems, the IDS is only as good as the latest signature database on the system. For additional information on Intrusion Detection Systems - http://en.wikipedia.org/wiki/Intrusion_detection_system Reference (s) used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 3623-3625, 3649-3654, 3666-3686). Auerbach Publications.
Kindle Edition.

QUESTION 459
What ensures that the control mechanisms correctly implement the security policy for the entire life cycle of an information system?

A. Accountability controls
B. Mandatory access controls
C. Assurance procedures
D. Administrative controls

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Controls provide accountability for individuals accessing information. Assurance procedures ensure that access control mechanisms correctly implement the security policy for the entire life cycle of an information system.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 33).

QUESTION 460
What IDS approach relies on a database of known attacks?

A. Signature-based intrusion detection
B. Statistical anomaly-based intrusion detection
C. Behavior-based intrusion detection
D. Network-based intrusion detection

Correct Answer: A

Explanation

Explanation/Reference:
Explanation: A weakness of the signature-based (or knowledge-based) intrusion detection approach is that only attack signatures that are stored in a database are detected. Network-based intrusion detection can either be signature-based or statistical anomaly-based (also called behavior-based).
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 49).

QUESTION 461
Which of the following is most likely to be useful in detecting intrusions?

A. Access control lists
B. Security labels
C. Audit trails
D. Information security policies

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: If audit trails have been properly defined and implemented, they will record information that can assist in detecting intrusions.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 4: Access Control (page 186).

QUESTION 462
Which conceptual approach to intrusion detection system is the most common?

A. Behavior-based intrusion detection
B. Knowledge-based intrusion detection
C. Statistical anomaly-based intrusion detection
D. Host-based intrusion detection

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: There are two conceptual approaches to intrusion detection. Knowledge-based intrusion detection uses a database of known vulnerabilities to look for current attempts to exploit them on a system and trigger an alarm if an attempt is found. The other approach, not as common, is called behaviour-based or statistical analysis-based. A host-based intrusion detection system is a common implementation of intrusion detection, not a conceptual approach. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 63).
Also: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 4: Access Control (pages 193-194).

QUESTION 463
Several analysis methods can be employed by an IDS, each with its own strengths and weaknesses, and their applicability to any given situation should be carefully considered. There are two basic IDS analysis methods that exists. Which of the basic method is more prone to false positive?

A. Pattern Matching (also called signature analysis)
B. Anomaly Detection
C. Host-based intrusion detection

D. Network-based intrusion detection

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Several analysis methods can be employed by an IDS, each with its own strengths and weaknesses, and their applicability to any given situation should be carefully considered.
There are two basic IDS analysis methods:
1. Pattern Matching (also called signature analysis), and
2. Anomaly detection
PATTERN MATCHING
Some of the first IDS products used signature analysis as their detection method and simply looked for known characteristics of an attack (such as specific packet sequences or text in the data stream) to produce an alert if that pattern was detected. If a new or different attack vector is used, it will not match a known signature and, thus, slip past the IDS.
ANOMALY DETECTION
Alternately, anomaly detection uses behavioral characteristics of a system's operation or network traffic to draw conclusions on whether the traffic represents a risk to the network or host.
Anomalies may include but are not limited to:
Multiple failed log-on attempts
Users logging in at strange hours
Unexplained changes to system clocks
Unusual error messages
Unexplained system shutdowns or restarts
Attempts to access restricted files
An anomaly-based IDS tends to produce more data because anything outside of the expected behavior is reported. Thus, they tend to report more false positives as expected behavior patterns change. An advantage to anomaly-based IDS is that, because they are based on behavior identification and not specific patterns of traffic, they are often able to detect new attacks that may be overlooked by a signature-based system. Often information from an anomaly-based IDS may be used to create a pattern for a signature-based IDS.
Host Based Intrusion Detection (HIDS)
HIDS is the implementation of IDS capabilities at the host level. Its most significant difference from NIDS is that related processes are limited to the boundaries of a single-host system. However, this presents advantages in effectively detecting objectionable activities because the IDS process is running directly on the host system, not just observing it from the network. This offers unfettered access to system logs, processes, system information, and device information, and virtually eliminates limits associated with encryption. The level of integration represented by HIDS increases the level of visibility and control at the disposal of the HIDS application.
Network Based Intrustion Detection (NIDS)
NIDS are usually incorporated into the network in a passive architecture, taking advantage of promiscuous mode access to the network. This means that it has visibility into every packet traversing the network segment. This allows the system to inspect packets and monitor sessions without impacting the network or the systems and applications utilizing the network. Below you have other ways that instrusion detection can be performed:
Stateful Matching Intrusion Detection
Stateful matching takes pattern matching to the next level. It scans for attack signatures in the context of a stream of traffic or overall system behavior rather than the individual packets or discrete system activities. For example, an attacker may use a tool that sends a volley of valid packets to a targeted system. Because all the packets are valid, pattern matching is nearly useless. However, the fact that a large volume of the packets was seen may, itself, represent a known or potential attack pattern. To evade attack, then, the attacker may send the packets from multiple locations with long wait periods between each transmission to either confuse the signature detection system or exhaust its session timing window. If the IDS service is tuned to record and analyze traffic over a long period of time it may detect such an attack. Because stateful matching also uses signatures, it too must be updated regularly and, thus, has some of the same limitations as pattern matching.
Statistical Anomaly-Based Intrusion Detection
The statistical anomaly-based IDS analyzes event data by comparing it to typical, known, or predicted traffic profiles in an effort to find potential security breaches. It attempts to identify suspicious behavior by analyzing event data and identifying patterns of entries that deviate from a predicted norm. This type of detection method can be very effective and, at a very high level, begins to take on characteristics seen in IPS by establishing an

expected baseline of behavior and acting on divergence from that baseline. However, there are some potential issues that may surface with a statistical IDS. Tuning the IDS can be challenging and, if not performed regularly, the system will be prone to false positives. Also, the definition of normal traffic can be open to interpretation and does not preclude an attacker from using normal activities to penetrate systems. Additionally, in a large, complex, dynamic corporate environment, it can be difficult, if not impossible, to clearly define "normal" traffic. The value of statistical analysis is that the system has the potential to detect previously unknown attacks. This is a huge departure from the limitation of matching previously known signatures. Therefore, when combined with signature matching technology, the statistical anomaly-based IDS can be very effective.

Protocol Anomaly-Based Intrusion Detection

A protocol anomaly-based IDS identifies any unacceptable deviation from expected behavior based on known network protocols. For example, if the IDS is monitoring an HTTP session and the traffic contains attributes that deviate from established HTTP session protocol standards, the IDS may view that as a malicious attempt to manipulate the protocol, penetrate a firewall, or exploit a vulnerability. The value of this method is directly related to the use of well-known or welldefined protocols within an environment. If an organization primarily uses well-known protocols (such as HTTP, FTP, or telnet) this can be an effective method of performing intrusion detection. In the face of custom or nonstandard protocols, however, the system will have more difficulty or be completely unable to determine the proper packet format. Interestingly, this type of method is prone to the same challenges faced by signature-based IDSs. For example, specific protocol analysis modules may have to be added or customized to deal with unique or new protocols or unusual use of standard protocols. Nevertheless, having an IDS that is intimately aware of valid protocol use can be very powerful when an organization employs standard implementations of common protocols.

Traffic Anomaly-Based Intrusion

Detection A traffic anomaly-based IDS identifies any unacceptable deviation from expected behavior based on actual traffic structure. When a session is established between systems, there is typically an expected pattern and behavior to the traffic transmitted in that session. That traffic can be compared to expected traffic conduct based on the understandings of traditional system interaction for that type of connection. Like the other types of anomaly-based IDS, traffic anomalybased IDS relies on the ability to establish "normal" patterns of traffic and expected modes of behavior in systems, networks, and applications. In a highly dynamic environment it may be difficult, if not impossible, to clearly define these parameters.

Reference(s) used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 3664-3686). Auerbach Publications. Kindle Edition.

and

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 3711-3734). Auerbach Publications. Kindle Edition.

and

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 3694-3711). Auerbach Publications. Kindle Edition.

QUESTION 464

In order to enable users to perform tasks and duties without having to go through extra steps it is important that the security controls and mechanisms that are in place have a degree of?

A. Complexity
B. Non-transparency
C. Transparency
D. Simplicity

Correct Answer: C
Explanation

Explanation/Reference:

Explanation: The security controls and mechanisms that are in place must have a degree of transparency. This enables the user to perform tasks and duties without having to go through extra steps because of the presence of the security controls. Transparency also does not let the user know too much about the controls, which helps prevent him from figuring out how to circumvent them. If the controls are too obvious, an attacker can figure out how to compromise them more easily. Security (more specifically, the implementation of most

security controls) has long been a sore point with users who are subject to security controls. Historically, security controls have been very intrusive to users, forcing them to interrupt their work flow and remember arcane codes or processes (like long passwords or access codes), and have generally been seen as an obstacle to getting work done. In recent years, much work has been done to remove that stigma of security controls as a detractor from the work process adding nothing but time and money. When developing access control, the system must be as transparent as possible to the end user. The users should be required to interact with the system as little as possible, and the process around using the control should be engineered so as to involve little effort on the part of the user. For example, requiring a user to swipe an access card through a reader is an effective way to ensure a person is authorized to enter a room. However, implementing a technology (such as RFID) that will automatically scan the badge as the user approaches the door is more transparent to the user and will do less to impede the movement of personnel in a busy area. In another example, asking a user to understand what applications and data sets will be required when requesting a system ID and then specifically requesting access to those resources may allow for a great deal of granularity when provisioning access, but it can hardly be seen as transparent. A more transparent process would be for the access provisioning system to have a role-based structure, where the user would simply specify the role he or she has in the organization and the system would know the specific resources that user needs to access based on that role. This requires less work and interaction on the part of the user and will lead to more accurate and secure access control decisions because access will be based on predefined need, not user preference.
When developing and implementing an access control system special care should be taken to ensure that the control is as transparent to the end user as possible and interrupts his work flow as little as possible.
The following answers were incorrect:
All of the other detractors were incorrect.
Reference(s) used for this question:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 6th edition. Operations Security, Page 1239-1240
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 25278- 25281). McGraw-Hill. Kindle Edition.
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Access Control ((ISC) 2 Press) (Kindle Locations 713-729). Auerbach Publications. Kindle Edition.

QUESTION 465
Which of the following is required in order to provide accountability?

A. Authentication
B. Integrity
C. Confidentiality
D. Audit trails

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Accountability can actually be seen in two different ways:
1) Although audit trails are also needed for accountability, no user can be accountable for their actions unless properly authenticated.
2) Accountability is another facet of access control. Individuals on a system are responsible for their actions. This accountability property enables system activities to be traced to the proper individuals. Accountability is supported by audit trails that record events on the system and network. Audit trails can be used for intrusion detection and for the reconstruction of past events. Monitoring individual activities, such as keystroke monitoring, should be accomplished in accordance with the company policy and appropriate laws. Banners at the log-on time should notify the user of any monitoring that is being conducted. The point is that unless you employ an appropriate auditing mechanism, you don't have accountability. Authorization only gives a user certain permissions on the network. Accountability is far more complex because it also includes intrusion detection, unauthorized actions by both unauthorized users and authorized users, and system faults. The audit trail provides the proof that unauthorized modifications by both authorized and unauthorized users took place. No proof, No accountability.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Page 50. The Shon Harris AIO book, 4th Edition, on Page 243

also states:
Auditing Capabilities ensures users are accountable for their actions, verify that the secutiy policies are enforced,
and can be used as investigation tools. Accountability is tracked by recording user, system, and application activities.
This recording is done through auditing functions and mechanisms within an operating sytem or application.
Audit trail contain information about operating System activities, application events, and user actions.

QUESTION 466
Which of the following is NOT a valid reason to use external penetration service firms rather than corporate resources?

A. They are more cost-effective
B. They offer a lack of corporate bias
C. They use highly talented ex-hackers
D. They ensure a more complete reporting

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Two points are important to consider when it comes to ethical hacking: integrity and independence.
By not using an ethical hacking firm that hires or subcontracts to ex-hackers of others who have criminal records, an entire subset of risks can be avoided by an organization. Also, it is not costeffective for a single firm to fund the effort of the ongoing research and development, systems development, and maintenance that is needed to operate state-of-the-art proprietary and open source testing tools and techniques.
External penetration firms are more effective than internal penetration testers because they are not influenced by any previous system security decisions, knowledge of the current system environment, or future system security plans. Moreover, an employee performing penetration testing might be reluctant to fully report security gaps. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Appendix F: The Case for Ethical Hacking (page 517).

QUESTION 467
Which of the following statements pertaining to ethical hacking is incorrect?

A. An organization should use ethical hackers who do not sell auditing, hardware, software, firewall, hosting, and/or networking services.
B. Testing should be done remotely to simulate external threats.
C. Ethical hacking should not involve writing to or modifying the target systems negatively.
D. Ethical hackers never use tools that have the potential of affecting servers or services.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: This means that many of the tools used for ethical hacking have the potential of exploiting vulnerabilities and causing disruption to IT system. It is up to the individuals performing the tests to be familiar with their use and to make sure that no such disruption can happen or at least shoudl be avoided.
The first step before sending even one single packet to the target would be to have a signed agreement with clear rules of engagement and a signed contract. The signed contract explains to the client the associated risks and the client must agree to them before you even send one packet to the target range. This way the client understand that some of the test could lead to interruption of service or even crash a server. The client signs that he is aware of such risks and willing to accept them.
The following are incorrect answers:
An organization should use ethical hackers who do not sell auditing, hardware, software, firewall, hosting, and/or networking services. An ethical hacking firm's independence can be questioned if they sell security solutions

at the same time as doing testing for the same client. There has to be independance between the judge (the tester) and the accuse (the client). Testing should be done remotely to simulate external threats Testing simulating a cracker from the Internet is often time one of the first test being done, this is to validate perimeter security. By performing tests remotely, the ethical hacking firm emulates the hacker's approach more realistically.

Ethical hacking should not involve writing to or modifying the target systems negatively. Even though ethical hacking should not involve negligence in writing to or modifying the target systems or reducing its response time, comprehensive penetration testing has to be performed using the most complete tools available just like a real cracker would.

Reference(s) used for this question:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Appendix F: The Case for Ethical Hacking (page 520).

QUESTION 468

The viewing of recorded events after the fact using a closed-circuit TV camera is considered a

A. Preventative control.

B. Detective control

C. Compensating control

D. Corrective control

Correct Answer: B

Explanation

Explanation/Reference:

Explanation: Detective security controls are like a burglar alarm. They detect and report an unauthorized or undesired event (or an attempted undesired event). Detective security controls are invoked after the undesirable event has occurred. Example detective security controls are log monitoring and review, system audit, file integrity checkers, and motion detection. Visual surveillance or recording devices such as closed circuit television are used in conjunction with guards in order to enhance their surveillance ability and to record events for future analysis or prosecution.

When events are monitored, it is considered preventative whereas recording of events is considered detective in nature.

Below you have explanations of other types of security controls from a nice guide produce by James Purcell (see reference below):

Preventive security controls are put into place to prevent intentional or unintentional disclosure, alteration, or destruction (D.A.D.) of sensitive information. Some example preventive controls follow:

Policy Unauthorized network connections are prohibited.

Firewall Blocks unauthorized network connections.

Locked wiring closet Prevents unauthorized equipment from being physically plugged into a network switch.

Notice in the preceding examples that preventive controls crossed administrative, technical, and physical categories discussed previously. The same is true for any of the controls discussed in this section.

Corrective security controls are used to respond to and fix a security incident. Corrective security controls also limit or reduce further damage from an attack. Examples follow:

Procedure to clean a virus from an infected system

A guard checking and locking a door left unlocked by a careless employee Updating firewall rules to block an attacking IP address Note that in many cases the corrective security control is triggered by a detective security control. Recovery security controls are those controls that put a system back into production after an incident. Most Disaster Recovery activities fall into this category. For example, after a disk failure, data is restored from a backup tape.

Directive security controls are the equivalent of administrative controls. Directive controls direct that some action be taken to protect sensitive organizational information. The directive can be in the form of a policy, procedure, or guideline.

Deterrent security controls are controls that discourage security violations. For instance, "Unauthorized Access Prohibited" signage may deter a trespasser from entering an area. The presence of security cameras might deter an employee from stealing equipment. A policy that states access to servers is monitored could deter unauthorized access. Compensating security controls are controls that provide an alternative to normal controls that cannot be used for some reason. For instance, a certain server cannot have antivirus software

installed because it interferes with a critical application. A compensating control would be to increase monitoring of that server or isolate that server on its own network segment. Note that there is a third popular taxonomy developed by NIST and described in NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems." NIST categorizes security controls into 3 classes and then further categorizes the controls within the classes into 17 families. Within each security control family are dozens of specific controls. The NIST taxonomy is not covered on the CISSP exam but is one the CISSP should be aware of if you are employed within the US federal workforce.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 10: Physical security (page 340).
and
CISSP Study Guide By Eric Conrad, Seth Misenar, Joshua Feldman, page 50-52 and
Security Control Types and Operational Security, James E. Purcell, http://www.giac.org/cissppapers/ 207.pdf

QUESTION 469
Controls provide accountability for individuals who are accessing sensitive information. This accountability is accomplished:

A. through access control mechanisms that require identification and authentication and through the audit function.
B. through logical or technical controls involving the restriction of access to systems and the protection of information.
C. through logical or technical controls but not involving the restriction of access to systems and the protection of information.
D. through access control mechanisms that do not require identification and authentication and do not operate through the audit function.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Controls provide accountability for individuals who are accessing sensitive information. This accountability is accomplished through access control mechanisms that require identification and authentication and through the audit function. These controls must be in accordance with and accurately represent the organization's security policy. Assurance procedures ensure that the control mechanisms correctly implement the security policy for the entire life cycle of an information system.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

QUESTION 470
Which of the following tools is less likely to be used by a hacker?

A. l0phtcrack
B. Tripwire
C. OphCrack
D. John the Ripper

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Tripwire is an integrity checking product, triggering alarms when important files (e.g.
system or configuration files) are modified.
This is a tool that is not likely to be used by hackers, other than for studying its workings in order to circumvent it.
Other programs are password-cracking programs and are likely to be used by security administrators as well as by hackers. More info regarding Tripwire available on the Tripwire, Inc.
Web Site.

NOTE:
The biggest competitor to the commercial version of Tripwire is the freeware version of Tripwire. You can get the Open Source version of Tripwire at the following URL:
http://sourceforge.net/projects/tripwire/

QUESTION 471
Why would anomaly detection IDSs often generate a large number of false positives?

A. Because they can only identify correctly attacks they already know about.
B. Because they are application-based are more subject to attacks.
C. Because they can't identify abnormal behavior.
D. Because normal patterns of user and system behavior can vary wildly.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Unfortunately, anomaly detectors and the Intrusion Detection Systems (IDS) based on them often produce a large number of false alarms, as normal patterns of user and system behavior can vary wildly. Being only able to identify correctly attacks they already know about isa characteristic of misuse detection (signature-based) IDSs. Application-based IDSs are a special subset of host-based IDSs that analyze the events transpiring within a software application. They are more vulnerable to attacks than host-based IDSs. Not being able to identify abnormal behavior would not cause false positives, since they are not identified. Source: DUPUIS, Cl?ment, Access Control Systems and Methodology CISSP Open Study Guide, version 1.0, march 2002 (page 92).

QUESTION 472
What is the essential difference between a self-audit and an independent audit?

A. Tools used
B. Results
C. Objectivity
D. Competence

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: To maintain operational assurance, organizations use two basic methods: system audits and monitoring. Monitoring refers to an ongoing activity whereas audits are one-time or periodic events and can be either internal or external. The essential difference between a selfaudit and an independent audit is objectivity, thus indirectly affecting the results of the audit. Internal and external auditors should have the same level of competence and can use the same tools.
Source: SWANSON, Marianne & GUTTMAN, Barbara, National Institute of Standards and Technology (NIST), NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996 (page 25).

QUESTION 473
A periodic review of user account management should not determine:

A. Conformity with the concept of least privilege.
B. Whether active accounts are still being used.
C. Strength of user-chosen passwords.
D. Whether management authorizations are up-to-date.

Correct Answer: C

Explanation

Explanation/Reference:
Explanation: Organizations should have a process for (1) requesting, establishing, issuing, and closing user accounts; (2) tracking users and their respective access authorizations; and (3) managing these functions. Reviews should examine the levels of access each individual has, conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up-todate, whether required training has been completed, and so forth. These reviews can be conducted on at least two levels: (1) on an application-by-application basis, or (2) on a system wide basis.
The strength of user passwords is beyond the scope of a simple user account management review, since it requires specific tools to try and crack the password file/database through either a dictionary or brute-force attack in order to check the strength of passwords.
Reference(s) used for this question:
SWANSON, Marianne & GUTTMAN, Barbara, National Institute of Standards and Technology (NIST), NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996 (page 28).

QUESTION 474
Due care is not related to:

A. Good faith
B. Prudent man
C. Profit
D. Best interest

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Officers and directors of a company are expected to act carefully in fulfilling their tasks. A director shall act in good faith, with the care an ordinarily prudent person in a like position would exercise under similar circumstances and in a manner he reasonably believes is in the best interest of the enterprise. The notion of profit would tend to go against the due care principle. Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 10: Law, Investigation, and Ethics (page 186).

QUESTION 475
Which of the following is not a preventive operational control?

A. Protecting laptops, personal computers and workstations.
B. Controlling software viruses.
C. Controlling data media access and disposal.
D. Conducting security awareness and technical training.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Conducting security awareness and technical training to ensure that end users and system users are aware of the rules of behaviour and their responsibilities in protecting the organization's mission is an example of a preventive management control, therefore not an operational control.
Source: STONEBURNER, Gary et al., NIST Special publication 800-30, Risk management Guide for Information Technology Systems, 2001 (page 37).

QUESTION 476
Which of the following questions are least likely to help in assessing controls covering audit trails?

A. Does the audit trail provide a trace of user actions?

B. Are incidents monitored and tracked until resolved?

C. Is access to online logs strictly controlled?

D. Is there separation of duties between security personnel who administer the access control function and those who administer the audit trail?

Correct Answer: B

Explanation

Explanation/Reference:

Explanation: Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide individual accountability, a means to reconstruct events, detect intrusions, and identify problems. Audit trail controls are considered technical controls. Monitoring and tracking of incidents is more an operational control related to incident response capability.

Reference(s) used for this question:

SWANSON, Marianne, NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001 (Pages A-50 to A-51). NOTE: NIST SP 800-26 has been superceded By: FIPS 200, SP 800-53, SP 800-53A You can find the new replacement at: http://csrc.nist.gov/publications/PubsSPs.html However, if you really wish to see the old standard, it is listed as an archived document at: http://csrc.nist.gov/publications/PubsSPArch.html

QUESTION 477

What setup should an administrator use for regularly testing the strength of user passwords?

A. A networked workstation so that the live password database can easily be accessed by the cracking program.

B. A networked workstation so the password database can easily be copied locally and processed by the cracking program.

C. A standalone workstation on which the password database is copied and processed by the cracking program.

D. A password-cracking program is unethical; therefore it should not be used.

Correct Answer: C

Explanation

Explanation/Reference:

Explanation: Poor password selection is frequently a major security problem for any system's security. Administrators should obtain and use password-guessing programs frequently to identify those users having easily guessed passwords.

Because password-cracking programs are very CPU intensive and can slow the system on which it is running, it is a good idea to transfer the encrypted passwords to a standalone (not networked) workstation. Also, by doing the work on a non-networked machine, any results found will not be accessible by anyone unless they have physical access to that system. Out of the four choice presented above this is the best choice. However, in real life you would have strong password policies that enforce complexity requirements and does not let the user choose a simple or short password that can be easily cracked or guessed. That would be the best choice if it was one of the choice presented. Another issue with password cracking is one of privacy. Many password cracking tools can avoid this by only showing the password was cracked and not showing what the password actually is. It is masking the password being used from the person doing the cracking. Source: National Security Agency, Systems and Network Attack Center (SNAC), The 60 Minute Network Security Guide, February 2002, page 8.

QUESTION 478

If an organization were to monitor their employees' e-mail, it should not:

A. Monitor only a limited number of employees.

B. Inform all employees that e-mail is being monitored.

C. Explain who can read the e-mail and how long it is backed up.

D. Explain what is considered an acceptable use of the e-mail system.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Monitoring has to be conducted is a lawful manner and applied in a consistent fashion; thus should be applied uniformly to all employees, not only to a small number. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 9: Law, Investigation, and Ethics (page 304).

QUESTION 479
Which of the following is the BEST way to detect software license violations?

A. Implementing a corporate policy on copyright infringements and software use.

B. Requiring that all PCs be diskless workstations.

C. Installing metering software on the LAN so applications can be accessed through the metered software.

D. Regularly scanning PCs in use to ensure that unauthorized copies of software have not been loaded on the PC.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The best way to prevent and detect software license violations is to regularly scan used PCs, either from the LAN or directly, to ensure that unauthorized copies of software have not been loaded on the PC.
Other options are not detective.
A corporate policy is not necessarily enforced and followed by all employees. Software can be installed from other means than floppies or CD-ROMs (from a LAN or even downloaded from the Internet) and software metering only concerns applications that are registered.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 3: Technical Infrastructure and Operational Practices (page 108).

QUESTION 480
In what way can violation clipping levels assist in violation tracking and analysis?

A. Clipping levels set a baseline for acceptable normal user errors, and violations exceeding that threshold will be recorded for analysis of why the violations occurred.

B. Clipping levels enable a security administrator to customize the audit trail to record only those violations which are deemed to be security relevant.

C. Clipping levels enable the security administrator to customize the audit trail to record only actions for users with access to user accounts with a privileged status.

D. Clipping levels enable a security administrator to view all reductions in security levels which have been made to user accounts which have incurred violations.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Companies can set predefined thresholds for the number of certain types of errors that will be allowed before the activity is considered suspicious. The threshold is a baseline for violation activities that may be normal for a user to commit before alarms are raised. This baseline is referred to as a clipping level.
The following are incorrect answers:
Clipping levels enable a security administrator to customize the audit trail to record only those violations which

are deemed to be security relevant. This is not the best answer, you would not record ONLY security relevant violations, all violations would be recorded as well as all actions performed by authorized users which may not trigger a violation. This could allow you to indentify abnormal activities or fraud after the fact.
Clipping levels enable the security administrator to customize the audit trail to record only actions for users with access to user accounts with a privileged status. It could record all security violations whether the user is a normal user or a privileged user. Clipping levels enable a security administrator to view all reductions in security levels which have been made to user accounts which have incurred violations. The keyword "ALL" makes this question wrong. It may detect SOME but not all of violations. For example, application level attacks may not be detected.
Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 1239). McGraw-Hill. Kindle Edition.
and
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 481
How often should a Business Continuity Plan be reviewed?

A. At least once a month
B. At least every six months
C. At least once a year
D. At least Quarterly

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: As stated in SP 800-34 Rev. 1:
To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. During the Operation/Maintenance phase of the SDLC, information systems undergo frequent changes because of shifting business needs, technology upgrades, or new internal or external policies. As a general rule, the plan should be reviewed for accuracy and completeness at an organizationdefined frequency (at least once a year for the purpose of the exam) or whenever significant changes occur to any element of the plan. Certain elements, such as contact lists, will require more frequent reviews.
Remember, there could be two good answers as specified above. Either once a year or whenever significant changes occur to the plan. You will of course get only one of the two presented within you exam.
Reference(s) used for this question:
NIST SP 800-34 Revision 1

QUESTION 482
Which of the following best describes what would be expected at a "hot site"?

A. Computers, climate control, cables and peripherals
B. Computers and peripherals
C. Computers and dedicated climate control systems.
D. Dedicated climate control systems

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: A Hot Site contains everything needed to become operational in the shortest amount of time.
The following answers are incorrect:
Computers and peripherals. Is incorrect because no mention is made of cables. You would not be fully operational without those.
Computers and dedicated climate control systems. Is incorrect because no mention is made of peripherals.

You would not be fully operational without those. Dedicated climate control systems. Is incorrect because no mentionis made of computers, cables and peripherals. You would not be fully operational without those. According to the OIG, a hot site is defined as a fully configured site with complete customer required hardware and software provided by the service provider. A hot site in the context of the CBK is always a RENTAL place. If you have your own site fully equipped that you make use of in case of disaster that would be called a redundant site or an alternate site. Wikipedia: "A hot site is a duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data."

OIG CBK, Business Continuity and Disaster Recovery Planning (pages 367 - 368) AIO, 3rd Edition, Business Continuity Planning (pages 709 - 714) AIO, 4th Edition, Business Continuity Planning , p 790. Wikipedia - http://en.wikipedia.org/wiki/Hot_site#Hot_Sites

QUESTION 483
Who should direct short-term recovery actions immediately following a disaster?

A. Chief Information Officer.
B. Chief Operating Officer.
C. Disaster Recovery Manager.
D. Chief Executive Officer.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The Disaster Recovery Manager should also be a member of the team that assisted in the development of the Disaster Recovery Plan. Senior-level management need to support the process but would not be involved with the initial process.
The following answers are incorrect:
Chief Information Officer. Is incorrect because the Senior-level management are the ones to authorize the recovery plan and process but during the initial recovery process they will most likely be heavily involved in other matters.
Chief Operating Officer. Is incorrect because the Senior-level management are the ones to authorize the recovery plan and process but during the initial recovery process they will most likely be heavily involved in other matters.
Chief Executive Officer. Is incorrect because the Senior-level management are the ones to authorize the recovery plan and process but during the initial recovery process they will most likely be heavily involved in other matters.

QUESTION 484
Which one of the following represents an ALE calculation?

A. single loss expectancy x annualized rate of occurrence.
B. gross loss expectancy x loss frequency.
C. actual replacement cost - proceeds of salvage.
D. asset value x loss expectancy.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Single Loss Expectancy (SLE) is the dollar amount that would be lost if there was a loss of an asset. Annualized Rate of Occurrence (ARO) is an estimated possibility of a threat to an asset taking place in one year (for example if there is a change of a flood occuring once in 10 years the ARO would be .1, and if there was a chance of a flood occuring once in 100 years then the ARO would be .01).
The following answers are incorrect:
gross loss expectancy x loss frequency. Is incorrect because this is a distractor. actual replacement cost - proceeds of salvage. Is incorrect because this is a distractor. asset value x loss expectancy. Is incorrect

because this is a distractor.

QUESTION 485
Prior to a live disaster test also called a Full Interruption test, which of the following is most important?

A. Restore all files in preparation for the test.
B. Document expected findings.
C. Arrange physical security for the test site.
D. Conduct of a successful Parallel Test

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: A live disaster test or Full interruption test is an actual simulation of the Disaster Recovery Plan. All operations are shut down and brought back online at the alternate site. This test poses the biggest threat to an organization and should not be performed until a successful Parallell Test has been conducted.
1. A Checklist test would be conducted where each of the key players will get a copy of the plan and they read it to make sure it has been properly developed for the specific needs of their departments.
2. A Structure Walk Through would be conducted next. This is when all key players meet together in a room and they walk through the test together to identify shortcoming and dependencies between department.
3. A simulation test would be next. In this case you go through a disaster scenario up to the point where you would move to the alternate site. You do not move to the alternate site and you learn from your mistakes and you improve the plan. It is the right time to find shortcomings.
4. A Parallell Test would be done. You go through a disaster scenario. You move to the alternate site and you process from both sites simultaneously.
5. A full interruption test would be conducted. You move to the alternate site and you resume processing at the alternate site.
The following answers are incorrect:
Restore all files in preparation for the test. Is incorrect because you would restore the files at the alternate site as part of the test not in preparation for the test. Document expected findings. Is incorrect because it is not the best answer. Documenting the expected findings won't help if you have not performed tests prior to a Full interruption test or live disaster test.
Arrange physical security for the test site. Is incorrect because it is not the best answer. why physical security for the test site is important if you have not performed a successful structured walk-through prior to performing a Full interruption test or live disaster test you might have some unexpected and disasterous results.

QUESTION 486
Which of the following should be emphasized during the Business Impact Analysis (BIA) considering that the BIA focus is on business processes?

A. Composition
B. Priorities
C. Dependencies
D. Service levels

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The Business Impact Analysis (BIA) identifies time-critical aspects of the critical business processes, and determines their maximum tolerable downtime. The BIA helps to Identify organization functions, the capabilities of each organization unit to handle outages, and the priority and sequence of functions and applications to be recovered, identify resources required for recovery of those areas and interdependencies
In performing the Business Impact Analysis (BIA) it is very important to consider what the dependencies are. You cannot bring a system up if it depends on another system to be operational. You need to look at not only

internal dependencies but external as well. You might not be able to get the raw materials for your business so dependencies are very important aspect of a BIA.
The BIA committee will not truly understand all business processes, the steps that must take place, or the resources and supplies these processes require. So the committee must gather this information from the people who do know-- department managers and specific employees throughout the organization. The committee starts by identifying the people who will be part of the BIA data-gathering sessions. The committee needs to identify how it will collect the data from the selected employees, be it through surveys, interviews, or workshops. Next, the team needs to collect the information by actually conducting surveys, interviews, and workshops. Data points obtained as part of the information gathering will be used later during analysis. It is important that the team members ask about how different tasks-- whether processes, transactions, or services, along with any relevant dependencies-- get accomplished within the organization.
The following answers are incorrect:
composition This is incorrect because it is not the best answer. While the make up of business may be important, if you have not determined the dependencies first you may not be able to bring the critical business processes to a ready state or have the materials on hand that are needed. priorities This is incorrect because it is not the best answer. While the priorities of processes are important, if you have not determined the dependencies first you may not be able to bring the critical business processes to a ready state or have the materials on hand that are needed. service levels This is incorrect because it is not the best answer. Service levels are not as important as dependencies.
Reference(s) used for this question:
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Business Continuity and Disaster Recovery Planning (Kindle Locations 188-191). . Kindle Edition.
and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 18562- 18568). McGraw-Hill. Kindle Edition.

QUESTION 487
Which of the following recovery plan test results would be most useful to management?

A. elapsed time to perform various activities.
B. list of successful and unsuccessful activities.
C. amount of work completed.
D. description of each activity.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: After a test has been performed the most useful test results for manangement would be knowing what worked and what didn't so that they could correct the mistakes where needed.
The following answers are incorrect:
elapsed time to perform various activities. This is incorrect because it is not the best answer, these results are not as useful as list of successful and unsuccessful activities would be to managment. amount of work completed. This is incorrect because it is not the best answer, these results are not as useful as list of successful and unsuccessful activities would be to managment. description of each activity. This is incorrect because it is not the best answer, these results are not as useful as list of successful and unsuccessful activities would be to managment.

QUESTION 488
Which of the following computer recovery sites is only partially equipped with processing equipment?

A. hot site
B. rolling hot site
C. warm site
D. cold site

Correct Answer: C

Explanation

Explanation/Reference:
Explanation: A warm site has some basic equipment or in some case almost all of the equipment but it is not sufficient to be operational without bringing in the last backup and in some cases more computers and other equipment.
The following answers are incorrect:
hot site. Is incorrect because a hot-site is fully configured with all the required hardware. The only thing missing is the last backup and you are up and running. Rolling hot site. Is incorrect because a rolling hot-site is fully configured with all the required hardware.
cold site. Is incorrect because a cold site has basically power, HVAC, basic cabling, but no or little as far as processing equipment is concerned. All other equipment must be brought to this site. It might take a week or two to reconstruct.

OIG CBK Business Continuity and Disaster Recovery Planning (pages 368 - 369)

QUESTION 489
Which of the following computer recovery sites is the least expensive and the most difficult to test?

A. non-mobile hot site
B. mobile hot site
C. warm site
D. cold site

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Is the least expensive because it is basically a structure with power and would be the most difficult to test because you would have to install all of the hardware infrastructure in order for it to be operational for the test.
The following answers are incorrect:
non-mobile hot site. Is incorrect because it is more expensive then a cold site and easier to test because all of the infrastructure is in place.
mobile hot site. Is incorrect because it is more expensive then a cold site and easier to test because all of the infrastructure is in place.
warm site. Is incorrect because it is more expensive then a cold site and easier to test because more of the infrastructure is in place.

QUESTION 490
Which of the following is the most important consideration in locating an alternate computing facility during the development of a disaster recovery plan?

A. It is unlikely to be affected by the same disaster.
B. It is close enough to become operational quickly.
C. It is close enough to serve its users.
D. It is convenient to airports and hotels.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: You do not want the alternate or recovery site located in close proximity to the original site because the same event that create the situation in the first place might very well impact that site also.
From NIST: "The fixed site should be in a geographic area that is unlikely to be negatively affected by the same disaster event (e.g., weather-related impacts or power grid failure) as the organization's primary site.
The following answers are incorrect:

It is close enough to become operational quickly. Is incorrect because it is not the best answer. You'd want the alternate site to be close but if it is too close the same event could impact that site as well.
It is close enough to serve its users. Is incorrect because it is not the best answer. You'd want the alternate site to be close to users if applicable, but if it is too close the same event could impact that site as well
It is convenient to airports and hotels. Is incorrect because it is not the best answer, it is more important that the same event does not impact the alternate site then convenience.

OIG CBK Business Continuity and Disaster Recovery Planning (pages 368 - 369) NIST document 800-34 pg 21

QUESTION 491
Contracts and agreements are often times unenforceable or hard to enforce in which of the following alternate facility recovery agreement?

A. hot site
B. warm site
C. cold site
D. reciprocal agreement

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: A reciprocal agreement is where two or more organizations mutually agree to provide facilities to the other if a disaster occurs. The organizations must have similiar hardware and software configurations. Reciprocal agreements are often not legally binding. Reciprocal agreements are not contracts and cannot be enforced. You cannot force someone you have such an agreement with to provide processing to you. Government regulators do not accept reciprocal agreements as valid disaster recovery sites. Cold sites are empty computer rooms consisting only of environmental systems, such as air conditioning and raised floors, etc. They do not meet the requirements of most regulators and boards of directors that the disaster plan be tested at least annually. Time Brokers promise to deliver processing time on other systems. They charge a fee, but cannot guaranty that processing will always be available, especially in areas that experienced multiple disasters.
With the exception of providing your own hot site, commercial hot sites provide the greatest protection. Most will allow you up to six weeks to restore your sites if you declare a disaster. They also permit an annual amount of time to test the Disaster Plan.

OIG CBK Business Continuity and Disaster Recovery Planning (pages 368 - 369) The following answers are incorrect:
hot site. Is incorrect because you have a contract in place stating what services are to be provided.
warm site. Is incorrect because you have a contract in place stating what services are to be provided.
cold site. Is incorrect because you have a contract in place stating what services are to be provided.

QUESTION 492
Organizations should not view disaster recovery as which of the following?

A. Committed expense.
B. Discretionary expense.
C. Enforcement of legal statutes.
D. Compliance with regulations.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Disaster Recovery should never be considered a discretionary expense. It is far too important a task. In order to maintain the continuity of the business Disaster Recovery should be a commitment of and by

the organization.
A discretionary fixed cost has a short future planning horizon--under a year. These types of costs arise from annual decisions of management to spend in specific fixed cost areas, such as marketing and research. DR would be an ongoing long term committment not a short term effort only.
A committed fixed cost has a long future planning horizon-- more than on year. These types of costs relate to a company's investment in assets such as facilities and equipment. Once such costs have been incurred, the company is required to make future payments.
The following answers are incorrect:
committed expense. Is incorrect because Disaster Recovery should be a committed expense. enforcement of legal statutes. Is incorrect because Disaster Recovery can include enforcement of legal statutes. Many organizations have legal requirements toward Disaster Recovery. compliance with regulations. Is incorrect because Disaster Recovery often means compliance with regulations. Many financial institutions have regulations requiring Disaster Recovery Plans and Procedures.

QUESTION 493
Which of the following groups represents the leading source of computer crime losses?

A. Hackers
B. Industrial saboteurs
C. Foreign intelligence officers
D. Employees

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: There are some conflicting figures as to which group is a bigger threat hackers or employees. Employees are still considered to the leading source of computer crime losses. Employees often have an easier time gaining access to systems or source code then ousiders or other means of creating computer crimes.
A word of caution is necessary: although the media has tended to portray the threat of cybercrime as existing almost exclusively from the outside, external to a company, reality paints a much different picture. Often the greatest risk of cybercrime comes from the inside, namely, criminal insiders. Information security professionals must be particularly sensitive to the phenomena of the criminal or dangerous insider, as these individuals usually operate under the radar, inside of the primarily outward/external facing security controls, thus significantly increasing the impact of their crimes while leaving few, if any, audit trails to follow and evidence for prosecution. Some of the large scale crimes committed agains bank lately has shown that Internal Threats are the worst and they are more common that one would think. The definition of what a hacker is can vary greatly from one country to another but in some of the states in the USA a hacker is defined as Someone who is using resources in a way that is not authorized. A recent case in Ohio involved an internal employee who was spending most of his day on dating website looking for the love of his life. The employee was taken to court for hacking the company resources.
The following answers are incorrect:
hackers. Is incorrect because while hackers represent a very large problem and both the frequency of attacks and overall losses have grown hackers are considered to be a small segment of combined computer fraudsters.
industrial saboteurs. Is incorrect because industrial saboteurs tend to go after trade secrets. While the loss to the organization can be great, they still fall short when compared to the losses created by employees. Often it is an employee that was involved in industrial sabotage. foreign intelligence officers. Is incorrect because the losses tend to be national secrets. You really can't put t cost on this and the number of frequency and occurances of this is less than that of employee related losses.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 22327-22331). Auerbach Publications. Kindle Edition.

QUESTION 494
Which of the following is the best reason for the use of an automated risk analysis tool?

A. Much of the data gathered during the review cannot be reused for subsequent analysis.
B. Automated methodologies require minimal training and knowledge of risk analysis.
C. Most software tools have user interfaces that are easy to use and does not require any training.
D. Information gathering would be minimized and expedited due to the amount of information already built into the tool.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The use of tools simplifies this process. Not only do they usually have a database of assests, threats, and vulnerabilities but they also speed up the entire process. Using Automated tools for performing a risk assessment can reduce the time it takes to perform them and can simplify the process as well. The better types of these tools include a wellresearched threat population and associated statistics. Using one of these tools virtually ensures that no relevant threat is overlooked, and associated risks are accepted as a consequence of the threat being overlooked.
In most situations, the assessor will turn to the use of a variety of automated tools to assist in the vulnerability assessment process. These tools contain extensive databases of specific known vulnerabilities as well as the ability to analyze system and network configuration information to predict where a particular system might be vulnerable to different types of attacks. There are many different types of tools currently available to address a wide variety of vulnerability assessment needs. Some tools will examine a system from the viewpoint of the network, seeking to determine if a system can be compromised by a remote attacker exploiting available services on a particular host system. These tools will test for open ports listening for connections, known vulnerabilities in common services, and known operating system exploits.
Michael Gregg says:
Automated tools are available that minimize the effort of the manual process. These programs enable users to rerun the analysis with different parameters to answer "what-ifs." They perform calculations quickly and can be used to estimate future expected losses easier than performing the calculations manually.
Shon Harris in her latest book says:
The gathered data can be reused, greatly reducing the time required to perform subsequent analyses. The risk analysis team can also print reports and comprehensive graphs to present to management.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 4655-4661). Auerbach Publications. Kindle Edition.
and
CISSP Exam Cram 2 by Michael Gregg
and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 2333- 2335). McGraw-Hill. Kindle Edition.
The following answers are incorrect:
Much of the data gathered during the review cannot be reused for subsequent analysis. Is incorrect because the data can be reused for later analysis. Automated methodologies require minimal training and knowledge of risk analysis. Is incorrect because it is not the best answer. While a minimal amount of training and knowledge is needed, the analysis should still be performed by skilled professionals. Most software tools have user interfaces that are easy to use and does not require any training. Is incorrect because it is not the best answer. While many of the user interfaces are easy to use it is better if the tool already has information built into it. There is always a training curve when any product is being used for the first time.

QUESTION 495
A deviation from an organization-wide security policy requires which of the following?

A. Risk Acceptance
B. Risk Assignment
C. Risk Reduction
D. Risk Containment

Correct Answer: A

Explanation

Explanation/Reference:
Explanation: A deviation from an organization-wide security policy requires you to manage the risk. If you deviate from the security policy then you are required to accept the risks that might occur.
In some cases, it may be prudent for an organization to simply accept the risk that is presented in certain scenarios. Risk acceptance is the practice of accepting certain risk(s), typically based on a business decision that may also weigh the cost versus the benefit of dealing with the risk in another way.
The OIG defines Risk Management as: This term characterizes the overall process. The first phase of risk assessment includes identifying risks, risk-reducing measures, and the budgetary impact of implementing decisions related to the acceptance, avoidance, or transfer of risk.
The second phase of risk management includes the process of assigning priority to, budgeting, implementing, and maintaining appropriate risk-reducing measures. Risk management is a continuous process of ever-increasing complexity. It is how we evaluate the impact of exposures and respond to them. Risk management minimizes loss to information assets due to undesirable events through identification, measurement, and control. It encompasses the overall security review, risk analysis, selection and evaluation of safeguards, cost-benefit analysis, management decision, and safeguard identification and implementation, along with ongoing effectiveness review.
Risk management provides a mechanism to the organization to ensure that executive management knows current risks, and informed decisions can be made to use one of the risk management principles: risk avoidance, risk transfer, risk mitigation, or risk acceptance. The 4 ways of dealing with risks are: Avoidance, Transfer, Mitigation, Acceptance The following answers are incorrect:
Risk assignment. Is incorrect because it is a distractor, assignment is not one of the ways to manage risk.
Risk reduction. Is incorrect because there was a deviation of the security policy. You could have some additional exposure by the fact that you deviated from the policy. Risk containment. Is incorrect because it is a distractor, containment is not one of the ways to manage risk.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 8882-8886). Auerbach Publications. Kindle Edition.
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 10206-10208). Auerbach Publications. Kindle Edition.

QUESTION 496
Which of the following is biggest factor that makes Computer Crimes possible?

A. The fraudster obtaining advanced training & special knowledge.
B. Victim carelessness.
C. Collusion with others in information processing.
D. System design flaws.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The biggest factor that makes Computer Crimes possible is Victim Carelessness. Awareness and education can reduce the chance of someone becomming a victim. The types and frequency of Computer Crimes are increasing at a rapid rate. Computer Crime was once mainly the result of insiders or disgruntled employees. Now just about everybody has access to the internet, professional criminals are taking advantage of this. Specialized skills are no longer needed and a search on the internet can provide a fraudster with a plethora of tools that can be used to perpetuate fraud. All too often carelessness leads to someone being a victim. People often use simple passwords or write them down in plain sight where they can be found by fraudsters. People throwing away papers loaded with account numbers, social security numbers, or other types of non-public personal information. There are phishing e-mail attempts where the fraudster tries to redirect a potential victim to a bogus site that resembles a legitimate site in an attempt to get the users' login ID and password, or other credentials. There is also social engineering. Awareness and training can help reduce the chance of someone becoming a victim.
The following answers are incorrect:

The fraudster obtaining advanced training and special knowledge. Is incorrect because training and special knowledge is not required. There are many tools widely available to fraudsters. Collusion with others in information processing. Is incorrect because as more and more people use computers in their daily lives, it is no longer necessary to have someone on the inside be a party to fraud attempts.
System design flaws. Is incorrect because while System design flaws are sometimes a factor in Computer Crimes more often then not it is victim carelessness that leads to Computer Crimes.

OIG CBK Legal, Regulations, Compliance and Investigations (pages 695 - 697)

QUESTION 497
Under United States law, an investigator's notebook may be used in court in which of the following scenarios?

A. When the investigator is unwilling to testify.
B. When other forms of physical evidence are not available.
C. To refresh the investigators memory while testifying.
D. If the defense has no objections.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: An investigator's notebook cannot be used as evidence is court. It can only be used by the investigator to refresh his memory during a proceeding, but cannot be submitted as evidence in any form.
The following answers are incorrect:
When the investigator is unwilling to testify. Is incorrect because the notebook cannot be submitted as evidence in any form.
When other forms of physical evidence are not available. Is incorrect because the notebook cannot be submitted as evidence in any form.
If the defense has no objections. Is incorrect because the notebook cannot be submitted as evidence in any form.

QUESTION 498
In addition to the Legal Department, with what company function must the collection of physical evidence be coordinated if an employee is suspected?

A. Human Resources
B. Industrial Security
C. Public Relations
D. External Audit Group

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: If an employee is suspected of causing an incident, the human resources department may be involved--for example, in assisting with disciplinary proceedings. Legal Department. The legal experts should review incident response plans, policies, and procedures to ensure their compliance with law and Federal guidance, including the right to privacy. In addition, the guidance of the general counsel or legal department should be sought if there is reason to believe that an incident may have legal ramifications, including evidence collection, prosecution of a suspect, or a lawsuit, or if there may be a need for a memorandum of understanding (MOU) or other binding agreements involving liability limitations for information sharing.
Public Affairs, Public Relations, and Media Relations. Depending on the nature and impact of an incident, a need may exist to inform the media and, by extension, the public.
The Incident response team members could include:
Management
Information Security
Legal / Human Resources

Public Relations
Communications
Physical Security
Network Security
Network and System Administrators
Network and System Security Administrators
Internal Audit
Events versus Incidents
An event is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt. Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data. This guide addresses only adverse events that are computer security- related, not those caused by natural disasters, power failures, etc.
A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.
Examples of incidents are:
An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
Users are tricked into opening a "quarterly report" sent via email that is actually malware; running the tool has infected their computers and established connections with an external host. An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.
A user provides or exposes sensitive information to others through peer-to-peer file sharing services.
The following answers are incorrect:
Industrial Security. Is incorrect because it is not the best answer, the human resource department must be involved with the collection of physical evidence if an employee is suspected. public relations. Is incorrect because it is not the best answer. It would be an important element to minimize public image damage but not the best choice for this question. External Audit Group. Is incorrect because it is not the best answer, the human resource department must be involved with the collection of physical evidence if an employee is suspected.
Reference(s) used for this question:
NIST Special Publication 800-61

QUESTION 499
To be admissible in court, computer evidence must be which of the following?

A. Relevant
B. Decrypted
C. Edited
D. Incriminating

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Before any evidence can be admissible in court, the evidence has to be relevant, material to the issue, and it must be presented in compliance with the rules of evidence. This holds true for computer evidence as well.
While there are no absolute means to ensure that evidence will be allowed and helpful in a court of law, information security professionals should understand the basic rules of evidence. Evidence should be relevant, authentic, accurate, complete, and convincing. Evidence gathering should emphasize these criteria.
As stated in CISSP for Dummies:
Because computer-generated evidence can sometimes be easily manipulated, altered , or tampered with, and because it's not easily and commonly understood, this type of evidence is usually considered suspect in a court of law. In order to be admissible, evidence must be Relevant: It must tend to prove or disprove facts that are relevant and material to the case. Reliable: It must be reasonably proven that what is presented as evidence is what was originally collected and that the evidence itself is reliable. This is accomplished, in part,

through proper evidence handling and the chain of custody. (We discuss this in the upcoming section "Chain of custody and the evidence life cycle.")
Legally permissible: It must be obtained through legal means. Evidence that's not legally permissible may include evidence obtained through the following means:
Illegal search and seizure: Law enforcement personnel must obtain a prior court order; however, non-law enforcement personnel, such as a supervisor or system administrator, may be able to conduct an authorized search under some circumstances. Illegal wiretaps or phone taps: Anyone conducting wiretaps or phone taps must obtain a prior court order.
Entrapment or enticement: Entrapment encourages someone to commit a crime that the individual may have had no intention of committing. Conversely, enticement lures someone toward certain evidence (a honey pot, if you will) after that individual has already committed a crime. Enticement is not necessarily illegal but does raise certain ethical arguments and may not be admissible in court.
Coercion: Coerced testimony or confessions are not legally permissible. Unauthorized or improper monitoring: Active monitoring must be properly authorized and conducted in a standard manner; users must be notified that they may be subject to monitoring.
The following answers are incorrect:
decrypted. Is incorrect because evidence has to be relevant, material to the issue, and it must be presented in compliance with the rules of evidence.
edited. Is incorrect because evidence has to be relevant, material to the issue, and it must be presented in compliance with the rules of evidence. Edited evidence violates the rules of evidence. incriminating. Is incorrect because evidence has to be relevant, material to the issue, and it must be presented in compliance with the rules of evidence.
Reference(s) used for this question:
CISSP STudy Guide (Conrad, Misenar, Feldman) Elsevier. 2012. Page 423 and
Mc Graw Hill, Shon Harris CISSP All In One (AIO), 6th Edition , Pages 1051-1056 and
CISSP for Dummies , Peter Gregory

QUESTION 500
The typical computer fraudsters are usually persons with which of the following characteristics?

A. They have had previous contact with law enforcement
B. They conspire with others
C. They hold a position of trust
D. They deviate from the accepted norms of society

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: These people, as employees, are trusted to perform their duties honestly and not take advantage of the trust placed in them.
The following answers are incorrect:
They have had previous contact with law enforcement. Is incorrect because most often it is a person that holds a position of trust and this answer implies they have a criminal background. This type of individual is typically not in a position of trust within an organization. They conspire with others. Is incorrect because they typically work alone, often as a form of retribution over a percieved injustice done to them.
They deviate from the accepted norms of society. Is incorrect because while the nature of fraudsters deviate from the norm, the fraudsters often hold a position of trust within the organization.

QUESTION 501
Once evidence is seized, a law enforcement officer should emphasize which of the following?

A. Chain of command
B. Chain of custody
C. Chain of control
D. Chain of communications

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: All people that handle the evidence from the time the crime was committed through the final disposition must be identified. This is to ensure that the evidence can be used and has not been tampered with.
The following answers are incorrect:
chain of command. Is incorrect because chain of command is the order of authority and does not apply to evidence.
chain of control. Is incorrect because it is a distractor. chain of communications. Is incorrect because it is a distractor.

QUESTION 502
Which of the following cannot be undertaken in conjunction or while computer incident handling is ongoing?

A. System development activity
B. Help-desk function
C. System Imaging
D. Risk management process

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: If Incident Handling is underway an incident has potentially been identified. At that point all use of the system should stop because the system can no longer be trusted and any changes could contaminate the evidence. This would include all System Development Activity. Every organization should have plans and procedures in place that deals with Incident Handling. Employees should be instructed what steps are to be taken as soon as an incident occurs and how to report it. It is important that all parties involved are aware of these steps to protect not only any possible evidence but also to prevent any additional harm. It is quite possible that the fraudster has planted malicous code that could cause destruction or even a Trojan Horse with a back door into the system. As soon as an incident has been identified the system can no longer be trusted and all use of the system should cease.
Shon Harris in her latest book mentions:
Although we commonly use the terms "event" and "incident" interchangeably, there are subtle differences between the two. An event is a negative occurrence that can be observed, verified, and documented, whereas an incident is a series of events that negatively affects the company and/ or impacts its security posture. This is why we call reacting to these issues "incident response" (or "incident handling"), because something is negatively affecting the company and causing a security breach.
Many types of incidents (virus, insider attack, terrorist attacks, and so on) exist, and sometimes it is just human error. Indeed, many incident response individuals have received a frantic call in the middle of the night because a system is acting "weird." The reasons could be that a deployed patch broke something, someone misconfigured a device, or the administrator just learned a new scripting language and rolled out some code that caused mayhem and confusion. When a company endures a computer crime, it should leave the environment and evidence unaltered and contact whomever has been delegated to investigate these types of situations. Someone who is unfamiliar with the proper process of collecting data and evidence from a crime scene could instead destroy that evidence, and thus all hope of prosecuting individuals, and achieving a conviction would be lost.
Companies should have procedures for many issues in computer security such as enforcement procedures, disaster recovery and continuity procedures, and backup procedures. It is also necessary to have a procedure for dealing with computer incidents because they have become an increasingly important issue of today's information security departments. This is a direct result of attacks against networks and information systems increasing annually. Even though we don't have specific numbers due to a lack of universal reporting and reporting in general, it is clear that the volume of attacks is increasing.
Just think about all the spam, phishing scams, malware, distributed denial-of-service, and other attacks you see on your own network and hear about in the news. Unfortunately, many companies are at a loss as to who to call or what to do right after they have been the victim of a cybercrime. Therefore, all companies should

have an incident response policy that indicates who has the authority to initiate an incident response, with supporting procedures set up before an incident takes place.
This policy should be managed by the legal department and security department. They need to work together to make sure the technical security issues are covered and the legal issues that surround criminal activities are properly dealt with. The incident response policy should be clear and concise. For example, it should indicate if systems can be taken offline to try to save evidence or if systems have to continue functioning at the risk of destroying evidence. Each system and functionality should have a priority assigned to it. For instance, if the file server is infected, it should be removed from the network, but not shut down. However, if the mail server is infected, it should not be removed from the network or shut down because of the priority the company attributes to the mail server over the file server. Tradeoffs and decisions will have to be made, but it is better to think through these issues before the situation occurs, because better logic is usually possible before a crisis, when there's less emotion and chaos. The Australian Computer Emergency Response Team's General Guidelines for Computer Forensics:
Keep the handling and corruption of original data to a minimum.
Document all actions and explain changes.
Follow the Five Rules for Evidence (Admissible, Authentic, Complete, Accurate, Convincing). · Bring in more experienced help when handling and/ or analyzing the evidence is beyond your knowledge, skills, or abilities.
Adhere to your organization's security policy and obtain written permission to conduct a forensics investigation.
Capture as accurate an image of the system(s) as possible while working quickly.
Be ready to testify in a court of law.
Make certain your actions are repeatable.
Prioritize your actions, beginning with volatile and proceeding to persistent evidence. Do not run any programs on the system(s) that are potential evidence. Act ethically and in good faith while conducting a forensics investigation, and do not attempt to do any harm.
The following answers are incorrect:
help-desk function. Is incorrect because during an incident, employees need to be able to communicate with a central source. It is most likely that would be the help-desk. Also the helpdesk would need to be able to communicate with the employees to keep them informed. system imaging. Is incorrect because once an incident has occured you should perform a capture of evidence starting with the most volatile data and imaging would be doen using bit for bit copy of storage medias to protect the evidence.
risk management process. Is incorrect because incident handling is part of risk management, and should continue.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 21468- 21476). McGraw-Hill. Kindle Edition.
and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 21096- 21121). McGraw-Hill. Kindle Edition.
and
NIST Computer Security incident handling http://csrc.nist.gov/publications/nistpubs/800-12/800- 12-html/ chapter12.html

QUESTION 503
Devices that supply power when the commercial utility power system fails are called which of the following?

A. power conditioners
B. uninterruptible power supplies
C. power filters
D. power dividers

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: From Shon Harris AIO Fifth Edition:
Protecting power can be done in three ways: through UPSs, power line conditioners, and backup sources. UPSs use battery packs that range in size and capacity. A UPS can be online or standby. Online UPS systems use AC line voltage to charge a bank of batteries. When in use, the UPS has an inverter that changes the DC

output from the batteries into the required AC form and that regulates the voltage as it powers computer devices.
Online UPS systems have the normal primary power passing through them day in and day out. They constantly provide power from their own inverters, even when the electric power is in proper use. Since the environment's electricity passes through this type of UPS all the time, the UPS device is able to quickly detect when a power failure takes place. An online UPS can provide the necessary electricity and picks up the load after a power failure much more quickly than a standby UPS.
Standby UPS devices stay inactive until a power line fails. The system has sensors that detect a power failure, and the load is switched to the battery pack. The switch to the battery pack is what causes the small delay in electricity being provided.
So an online UPS picks up the load much more quickly than a standby UPS, but costs more of course.

QUESTION 504
Within the realm of IT security, which of the following combinations best defines risk?

A. Threat coupled with a breach
B. Threat coupled with a vulnerability
C. Vulnerability coupled with an attack
D. Threat coupled with a breach of security

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The
Answer: Threat coupled with a vulnerability. Threats are circumstances or actions with the ability to harm a system. They can destroy or modify data or result an a DoS. Threats by themselves are not acted upon unless there is a vulnerability that can be taken advantage of. Risk enters the equation when a vulnerability (Flaw or weakness) exists in policies, procedures, personnel management, hardware, software or facilities and can be exploited by a threat agent. Vulnerabilities do not cause harm, but they leave the system open to harm. The combination of a threat with a vulnerability increases the risk to the system of an intrusion.
The following answers are incorrect:
Threat coupled with a breach. A threat is the potential that a particular threat-source will take advantage of a vulnerability. Breaches get around security. It does not matter if a breach is discovered or not, it has still occured and is not a risk of something occuring. A breach would quite often be termed as an incident or intrusion.
Vulnerability coupled with an attack. Vulnerabilities are weaknesses (flaws) in policies, procedures, personnel management, hardware, software or factilities that may result in a harmful intrusion to an IT system. An attack takes advantage of the flaw or vulnerability. Attacks are explicit attempts to violate security, and are more than risk as they are active. Threat coupled with a breach of security. This is a detractor. Although a threat agent may take advantage of (Breach) vulnerabilities or flaws in systems security. A threat coupled with a breach of security is more than a risk as this is active.
The following reference(s) may be used to research the question NO: s in this question:
ISC2 OIG, 2007 p. 66-67
Shon Harris AIO v3 p. 71-72

QUESTION 505
Which of the following backup sites is the most effective for disaster recovery?

A. Time brokers
B. Hot sites
C. Cold sites
D. Reciprocal Agreement

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: A hot site has the equipment, software and communications capabilities to facilitate a recovery within a few minutes or hours following the notification of a disaster to the organization's primary site. With the exception of providing your own hot site, commercial hot sites provide the greatest protection. Most will allow you up to six weeks to restore your sites if you declare a disaster. They also permit an annual amount of time to test the Disaster Plan.
The following answers are incorrect:
Cold sites. Cold sites are empty computer rooms consisting only of environmental systems, such as air conditioning and raised floors, etc. They do not meet the requirements of most regulators and boards of directors that the disaster plan be tested at least annually. Reciprocal Agreement. Reciprocal agreements are not contracts and cannot be enforced. You cannot force someone you have such an agreement with to provide processing to you. Government regulators do not accept reciprocal agreements as valid disaster recovery backup sites.
Time Brokers. Time Brokers promise to deliver processing time on other systems. They charge a fee, but cannot guaranty that processing will always be available, especially in areas that experienced multiple disasters.
The following reference(s) were/was used to create this question:
ISC2 OIG, 2007 p368
Shon Harris AIO v3. p.710

QUESTION 506
Which of the following is NOT a transaction redundancy implementation?

A. on-site mirroring
B. Electronic Vaulting
C. Remote Journaling
D. Database Shadowing

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Three concepts are used to create a level of fault tolerance and redundancy in transaction processing.
They are Electronic vaulting, remote journaling and database shadowing provide redundancy at the transaction level.
Electronic vaulting is accomplished by backing up system data over a network. The backup location is usually at a separate geographical location known as the vault site. Vaulting can be used as a mirror or a backup mechanism using the standard incremental or differential backup cycle. Changes to the host system are sent to the vault server in real-time when the backup method is implemented as a mirror. If vaulting updates are recorded in real-time, then it will be necessary to perform regular backups at the off-site location to provide recovery services due to inadvertent or malicious alterations to user or system data. Journaling or Remote Journaling is another technique used by database management systems to provide redundancy for their transactions. When a transaction is completed, the database management system duplicates the journal entry at a remote location. The journal provides sufficient detail for the transaction to be replayed on the remote system. This provides for database recovery in the event that the database becomes corrupted or unavailable. There are also additional redundancy options available within application and database software platforms. For example, database shadowing may be used where a database management system updates records in multiple locations. This technique updates an entire copy of the database at a remote location.
Reference used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 20403-20407). Auerbach Publications. Kindle Edition.
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 20375-20377). Auerbach Publications. Kindle Edition.

QUESTION 507
Which of the following steps is NOT one of the eight detailed steps of a Business Impact Assessment (BIA):

A. Notifying senior management of the start of the assessment.
B. Creating data gathering techniques.
C. Identifying critical business functions.
D. Calculating the risk for each different business function.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Source: HARRIS, S., CISSP All- In-One Exam Guide, 3rd. Edition, 2005, Chapter 9, Page 701.
There have been much discussion about the steps of the BIA and I struggled with this before deciding to scrape the question about "the four steps," and re-write the question using the AIO for a reference. This question should be easy.... if you know all eight steps.
The eight detailed and granular steps of the BIA are:
1. Select Individuals to interview for the data gathering.
2. Create data gathering techniques (surveys, questionnaires, qualitative and quantitative approaches).
3. Identify the company's critical business functions.
4. Identify the resources that these functions depend upon.
5. Calculate how long these functions can survive without these resources.
6. Identify vulnerabilities and the threats to these functions.
7. Calculate risk for each of the different business functions.
8. Document findings and report them to management.
Shon goes on to cover each step in Chapter 9.

QUESTION 508
Which of the following results in the most devastating business interruptions?

A. Loss of Hardware/Software
B. Loss of Data
C. Loss of Communication Links
D. Loss of Applications

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Source: Veritas eLearning CD - Introducing Disaster Recovery Planning, Chapter 1. All of the others can be replaced or repaired. Data that is lost and was not backed up, cannot be restored.

QUESTION 509
Which of the following is the most critical item from a disaster recovery point of view?

A. Data
B. Hardware/Software
C. Communication Links
D. Software Applications

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The most important point is ALWAYS the data. Everything else can be replaced or repaired.
Data MUST be backed up, backups must be regularly tested, because once it is truly lost, it is lost forever.
The goal of disaster recovery is to minimize the effects of a disaster or disruption. It means taking the necessary steps to ensure that the resources, personnel, and business processes are able to resume

operation in a timely manner . This is different from continuity planning, which provides methods and procedures for dealing with longer-term outages and disasters. The goal of a disaster recovery plan is to handle the disaster and its ramifications right after the disaster hits; the disaster recovery plan is usually very information technology (IT) focused. A disaster recovery plan (DRP) is carried out when everything is still in emergency mode, and everyone is scrambling to get all critical systems back online.
Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 887). McGraw-Hill.
Kindle Edition.
and
Veritas eLearning CD - Introducing Disaster Recovery Planning, Chapter 1.

QUESTION 510
Which of the following is defined as the most recent point in time to which data must be synchronized without adversely affecting the organization (financial or operational impacts)?

A. Recovery Point Objective
B. Recovery Time Objective
C. Point of Time Objective
D. Critical Time Objective

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The recovery point objective (RPO) is the maximum acceptable level of data loss following an unplanned "event", like a disaster (natural or man-made), act of crime or terrorism, or any other business or technical disruption that could cause such data loss. The RPO represents the point in time, prior to such an event or incident, to which lost data can be recovered (given the most recent backup copy of the data).
The recovery time objective (RTO) is a period of time within which business and / or technology capabilities must be restored following an unplanned event or disaster. The RTO is a function of the extent to which the interruption disrupts normal operations and the amount of revenue lost per unit of time as a result of the disaster.
These factors in turn depend on the affected equipment and application(s). Both of these numbers represent key targets that are set by key businesses during business continuity and disaster recovery planning; these targets in turn drive the technology and implementation choices for business resumption services, backup / recovery / archival services, and recovery facilities and procedures.
Many organizations put the cart before the horse in selecting and deploying technologies before understanding the business needs as expressed in RPO and RTO; IT departments later bear the brunt of user complaints that their service expectations are not being met. Defining the RPO and RTO can avoid that pitfall, and in doing so can also make for a compelling business case for recovery technology spending and staffing.
For the CISSP candidate studying for the exam, there are no such objectives for "point of time," and "critical time." Those two answers are simply detracters. http://www.wikibon.org/Recovery_point_objective_/_recovery_time_objective_strategy

QUESTION 511
Valuable paper insurance coverage does not cover damage to which of the following?

A. Inscribed, printed and Written documents
B. Manuscripts
C. Records
D. Money and Securities

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: All businesses are driven by records. Even in today's electronic society businesses generate

mountains of critical documents everyday. Invoices, client lists, calendars, contracts, files, medical records, and innumerable other records are generated every day. Stop and ask yourself what happens if your business lost those documents today. Valuable papers business insurance coverage provides coverage to your business in case of a loss of vital records. Over the years policy language has evolved to include a number of different types of records. Generally, the policy will cover "written, printed, or otherwise inscribed documents and records, including books, maps, films, drawings, abstracts, deeds, mortgages, and manuscripts." But, read the policy coverage carefully. The policy language typically "does not mean "money" or "securities," converted data,programs or instructions used in your data processing operations, including the materials on which the data is recorded." The coverage is often included as a part of property insurance or as part of a small business owner policy. For example, a small business owner policy includes in many cases valuable papers coverage up to $25,000.

It is important to realize what the coverage actually entails and, even more critical, to analyze your business to determine what it would cost to replace records. The coverage pays for the loss of vital papers and the cost to replace the records up to the limit of the insurance and after application of any deductible. For example, the insurer will pay to have waterlogged papers dried and reproduced (remember, fires are put out by water and the fire department does not stop to remove your book keeping records). The insurer may cover temporary storage or the cost of moving records to avoid a loss. For some businesses, losing customer lists, some business records, and contracts, can mean the expense and trouble of having to recreate those documents, but is relatively easy and a low level risk and loss. Larger businesses and especially professionals (lawyers, accountants, doctors) are in an entirely separate category and the cost of replacement of documents is much higher. Consider, in analyzing your business and potential risk, what it would actually cost to reproduce your critical business records. Would you need to hire temporary personnel? How many hours of productivity would go into replacing the records? Would you need to obtain originals? Would original work need to be recreated (for example, home inspectors, surveyors, cartographers)? Often when a business owner considers the actual cost related to the reproduction of records, the owner quickly realizes that their business insurance policy limits for valuable papers coverage is woefully inadequate.

Insurers (and your insurance professional)will often suggest higher coverages for valuable papers. The extra premium is often worth the cost and should be considered. Finally, most policies will require records to be protected. You need to review your declarations pages and speak with your insurer to determine what is required. Some insurers may offer discounted coverage if there is a document retention and back up plan in place and followed. There are professional organizations that can assist your business in designing a records management policy to lower the risk (and your premiums). For example, ARMA International has been around since 1955 and its members consist of some of the top document retention and storage companies.

Reference(s) used for this question:

http://businessinsure.about.com/od/propertyinsurance/f/vpcov.htm

QUESTION 512

Which of the following is covered under Crime Insurance Policy Coverage?

A. Inscribed, printed and Written documents

B. Manuscripts

C. Accounts Receivable

D. Money and Securities

Correct Answer: D

Explanation

Explanation/Reference:

Explanation: Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, Property Insurance overview, Page 589.

QUESTION 513

If your property Insurance has Actual Cash Valuation (ACV) clause, your damaged property will be compensated based on:

A. Value of item on the date of loss

B. Replacement with a new item for the old one regardless of condition of lost item

C. Value of item one month before the loss

D. Value of item on the date of loss plus 10 percent

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: This is called the Actual Cash Value (ACV) or Actual Cost Valuation (ACV) All of the other answers were only detractors. Below you have an explanation of the different types of valuation you could use. It is VERY important for you to validate with your insurer which one applies to you as you could have some very surprising finding the day you have a disaster that takes place.
Replacement Cost
Property replacement cost insurance promises to replace old with new. Generally, replacement of a building must be done on the same premises and used for the same purpose, using materials comparable to the quality of the materials in the damaged or destroyed property. There are some other limitations to this promise. For example, the cost of repairs or replacement for buildings
doesn't include the increased cost associated with building codes or other laws controlling how buildings must be built today. An endorsement adding coverage for the operation of Building Codes and the increased costs associated with complying with them is available separately -- usually for additional premium.
In addition, some insurance underwriters will only cover certain property on a depreciated value (actual cash value -- ACV) basis even when attached to the building. This includes awnings and floor coverings, appliances for refrigerating, ventilating, cooking, dishwashing, and laundering. Depreciated value also applies to outdoor equipment or furniture.
Actual Cash Value (ACV)
The ACV is the default valuation clause for commercial property insurance. It is also known as depreciated value, but this is not the same as accounting depreciated value. The actual cash value is determined by first calculating the replacement value of the property. The next step involves estimating the amount to be subtracted, which reflects the building's age, wear, and tear.
This amount deducted from the replacement value is known as depreciation. The amount of depreciation is reduced by inflation (increased cost of replacing the property); regular maintenance; and repair (new roofs, new electrical systems, etc.) because these factors reduce the effective age of the buildings.
The amount of depreciation applicable is somewhat subjective and certainly subject to negotiation. In fact, there is often disagreement and a degree of uncertainty over the amount of depreciation applicable to a particular building.
Given this reality, property owners should not leave the determination of depreciation to chance or wait until suffering
a property loss to be concerned about it. Every three to five years, property owners should obtain a professional appraisal of the replacement value and depreciated value of the buildings. The ACV valuation is an option for directors to consider when certain buildings are in need of repair, or budget constraints prevent insuring all of your facilities on a replacement cost basis. There are other valuation options for property owners to consider as well.
Functional Replacement Cost
This valuation method has been available for some time but has not been widely used. It is beginning to show up on property insurance policies imposed by underwriters with concerns about older, buildings. It can also be used for buildings, which are functionally obsolete. This method provides for the replacement of a building with similar property that performs the same function, using less costly material. The endorsement includes coverage for building codes automatically.
In the event of a loss, the insurance company pays the smallest of four payment options.
1. In the event of a total loss, the insurer could pay the limit of insurance on the building or the cost to replace the building on the same (or different) site with a payment that is "functionally equivalent."
2. In the event of a partial loss, the insurance company could pay the cost to repair or replace the damaged portion in the same architectural style with less costly material (if available).
3. The insurance company could also pay the amount actually spent to demolish the undamaged portion of the building and clear the site if necessary.
4. The fourth payment option is to pay the amount actually spent to repair, or replace the building using less costly materials, if available (Hillman and McCracken 1997). Unlike the replacement cost valuation method, which excluded certain fixtures and personal property used to service the premises, this endorsement provides functional replacement cost coverage for these items (awnings, floor coverings, appliances, etc.) (Hillman nd McCracken 1997).

As in the standard replacement cost value option, the insured can elect not to repair or replace the property. Under these circumstances the company pays the smallest of the following:
1. The Limit of Liability
2. The "market value" (not including the value of the land) at the time of the loss. The endorsement defines "market value" as the price which the property might be expected to realize if ffered for sale in fair market."
3. A modified form of ACV (the amount to repair or replace on he same site with less costly material and in the same architectural tyle, less depreciation) (Hillman and McCracken 1997).
Agreed Value or Agreed Amount
Agreed value or agreed amount is not a valuation method. Instead, his term refers to a waiver of the coinsurance clause in the property insurance policy. Availability of this coverage feature varies among insurers but, it is usually available only when the underwriter has proof (an independent appraisal, or compliance with an insurance company valuation model) of the value of your property.
When do I get paid?
Generally, the insurance company will not pay a replacement cost settlement until the property that was damaged or destroyed is actually repaired or replaced as soon as reasonably possible after the loss.
Under no circumstances will the insurance company pay more than your limit of insurance or more than the actual amount you spend to repair or replace the damaged property if this amount is less than the limit of insurance.
Replacement cost insurance terms give the insured the option of settling the loss on an ACV basis. This option may be exercised if you don't plan to replace the building or if you are faced with a significant coinsurance penalty on a replacement cost settlement.

http://www.schirickinsurance.com/resources/value2005.pdf and
TIPTON, Harold F. & KRAUSE, MICKI
Information Security Management Handbook, 4th Edition, Volume 1 Property Insurance overview, Page 587.

QUESTION 514
If your property Insurance has Replacement Cost Valuation (RCV) clause your damaged property will be compensated:

A. Based on the value of item on the date of loss
B. Based on new, comparable, or identical item for old regardless of condition of lost item
C. Based on value of item one month before the loss
D. Based on the value listed on the Ebay auction web site

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: RCV is the maximum amount your insurance company will pay you for damage to covered property before deducting for depreciation. The RCV payment is based on the current cost to replace your property with new, identical or comparable property.
The other choices were detractor:
Application and definition of the insurance terms Replacement Cost Value (RCV), Actual Cash Value (ACV) and depreciation can be confusing. It's important that you understand the terms to help settle your claim fairly.
An easy way to understand RCV and ACV is to think in terms of "new" and "used." Replacement cost is the item's current price, new. "What will it cost when I replace it?" Actual cash is the item's used price, old. "How much money is it worth since I used it for five years?"
Hold Back
Most policies only pay the Actual Cash Value upfront, and then they pay you the "held back" depreciation after you incur the expense to repair or replace your personal property items. NOTE: You must remember to send documentation to the insurance company proving you've incurred the additional expense you will be reimbursed.
Actual Cash Value (ACV)
ACV is the amount your insurance company will pay you for damage to covered property after deducting for depreciation. ACV is the replacement cost of a new item, minus depreciation. If stated as a simple equation, ACV could be defined as follows: ACV=RCV-Depreciation Unfortunately, ACV is not always as easy to agree upon as a simple math equation. The ACV can also be calculated as the price a willing buyer would pay for

your used item.
Depreciation
Depreciation (sometimes called "hold back") is defined as the "loss in value from all causes, including age, and wear and tear." Although the definition seems to be clear, in our experience, value" as a real-world application is clearly subjective and varies widely. We have seen the same adjuster apply NO depreciation (100 percent value) on one claim and 40 percent depreciation almost half value) on an almost identical claim.
This shows that the process of applying depreciation is subjective and clearly negotiable.
Excessive Depreciation
When the insurance company depreciates more than they should, it is called "Excessive depreciation." Although not ethical, it is very common. Note any items that have excessive depreciation and write a letter to your insurance company.

http://carehelp.org/downloads/category/1-insurance-handouts.html?download=17%3Ahandout08- rcv-and-acv and
http://www.schirickinsurance.com/resources/value2005.pdf and
TIPTON, Harold F. & KRAUSE, MICKI, information Security Management Handbook, 4th Edition, Volume 1 Property Insurance overview, Page 587.

QUESTION 515
A momentary power outage is a:

A. spike
B. blackout
C. surge
D. fault

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: A momentary power outage is a fault.
Power Excess
Spike --> Too much voltage for a short period of time.
Surge --> Too much voltage for a long period of time.
Power Loss
Fault --> A momentary power outage.
Blackout --> A long power interruption.
Power Degradation
Sag or Dip --> A momentary low voltage.
Brownout --> A prolonged power supply that is below normal voltage.
Reference(s) used for this question:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 3rd. Edition McGraw-Hill/Osborne, 2005, page 368.
and
https://en.wikipedia.org/wiki/Power_quality

QUESTION 516
A momentary high voltage is a:

A. spike
B. blackout
C. surge
D. fault

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Too much voltage for a short period of time is a spike. Too much voltage for a long period of time is a surge. Not enough voltage for a short period of time is a sag or dip Not enough voltage for a long period of time is brownout A short power interruption is a fault
A long power interruption is a blackout
You MUST know all of the power issues above for the purpose of the exam. From: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 3rd. Edition McGraw- Hill/Osborne, 2005, page 368.

QUESTION 517
A momentary low voltage, from 1 cycle to a few seconds, is a:

A. spike
B. blackout
C. sag
D. fault

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: A momentary low voltage is a sag. A synonym would be a dip.
Risks to electrical power supply:
POWER FAILURE
Blackout: complete loss of electrical power
Fault: momentary power outage
POWER DEGRADATION
Brownout: an intentional reduction of voltage by the power company.
Sag/dip: a short period of low voltage
POWER EXCESS
Surge: Prolonged rise in voltage
Spike: Momentary High Voltage
In-rush current: the initial surge of current required by a load before it reaches normal operation. Transient: line noise or disturbance is superimposed on the supply circuit and can cause fluctuations in electrical power
Refence(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 462). McGraw-Hill.
Kindle Edition.

QUESTION 518
A prolonged high voltage is a:

A. spike
B. blackout
C. surge
D. fault

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: A prolonged high voltage is a surge.
From: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 3rd. Edition McGraw- Hill/Osborne, 2005, page 368.

QUESTION 519
A prolonged complete loss of electric power is a:

A. brownout

B. blackout
C. surge
D. fault

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: A prolonged power outage is a blackout.
From: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 3rd. Edition McGraw- Hill/Osborne, 2005, page 368.

QUESTION 520
A prolonged power supply that is below normal voltage is a:

A. brownout
B. blackout
C. surge
D. fault

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: A prolonged power supply that is below normal voltage is a brownout. From: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 3rd. Edition McGraw- Hill/Osborne, 2005, page 368.

QUESTION 521
Because ordinary cable introduces a toxic hazard in the event of fire, special cabling is required in a separate area provided for air circulation for heating, ventilation, and air-conditioning (sometimes referred to as HVAC) and typically provided in the space between the structural ceiling and a dropdown ceiling. This area is referred to as the:

A. smoke boundry area
B. fire detection area
C. Plenum area
D. Intergen area

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: In building construction, a plenum (pronounced PLEH-nuhm, from Latin meaning full) is a separate space provided for air circulation for heating, ventilation, and air-conditioning (sometimes referred to as HVAC) and typically provided in the space between the structural ceiling and a drop-down ceiling. A plenum may also be under a raised floor. In buildings with computer installations, the plenum space is often used to house connecting communication cables. Because ordinary cable introduces a toxic hazard in the event of fire, special plenum cabling is required in plenum areas.
Source: http://searchdatacenter.techtarget.com/sDefinition/0,,sid80_gci213716,00.html

QUESTION 522
What is the Maximum Tolerable Downtime (MTD)?

A. Maximum elapsed time required to complete recovery of application data
B. Minimum elapsed time required to complete recovery of application data

C. Maximum elapsed time required to move back to primary site after a major disruption

D. It is maximum delay businesses can tolerate and still remain viable

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The Maximum Tolerable Downtime (MTD) is the maximum length of time a BUSINESS FUNCTION can endure without being restored, beyond which the BUSINESS is no longer viable
NIST SAYS:
The ISCP Coordinator should analyze the supported mission/business processes and with the process owners, leadership and business managers determine the acceptable downtime if a given process or specific system data were disrupted or otherwise unavailable. Downtime can be identified in several ways.
Maximum Tolerable Downtime (MTD). The MTD represents the total amount of time the system owner/ authorizing official is willing to accept for a mission/business process outage or disruption and includes all impact considerations. Determining MTD is important because it could leave contingency planners with imprecise direction on selection of an appropriate recovery method, and the depth of detail which will be required when developing recovery procedures, including their scope and content.
Other BCP and DRP terms you must be familiar with are:
Recovery Time Objective (RTO). RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/ business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD. When it is not feasible to immediately meet the RTO and the MTD is inflexible, a Plan of Action and Milestone should be initiated to document the situation and plan for its mitigation.
Recovery Point Objective (RPO). The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data can be recovered (given the most recent backup copy of the data) after an outage. Unlike RTO, RPO is not considered as part of MTD. Rather, it is a factor of how much data loss the mission/business process can tolerate during the recovery process. Because the RTO must ensure that the MTD is not exceeded, the RTO must normally be shorter than the MTD. For example, a system outage may prevent a particular process from being completed, and because it takes time to reprocess the data, that additional processing time must be added to the RTO to stay within the time limit established by the MTD.
References used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Page 276.
and
http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

QUESTION 523
Out of the steps listed below, which one is not one of the steps conducted during the Business Impact Analysis (BIA)?

A. Alternate site selection

B. Create data-gathering techniques

C. Identify the company's critical business functions

D. Select individuals to interview for data gathering

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Selecting and Alternate Site would not be done within the initial BI A. It would be
done at a later stage of the BCP and DRP recovery effort. All of the other choices were steps that would be conducted during the BI
A. See below the list of steps that would be done during the BIA. A BIA (business impact analysis) is considered a functional analysis, in which a team collects data through interviews and documentary sources; documents business functions, activities, and transactions ; develops a hierarchy of business functions; and finally applies a classification scheme to indicate each individual function's criticality level.

BIA Steps
1. Select individuals to interview for data gathering.
2. Create data-gathering techniques (surveys, questionnaires, qualitative and quantitative approaches).
3. Identify the company's critical business functions.
4. Identify the resources these functions depend upon.
5. Calculate how long these functions can survive without these resources.
6. Identify vulnerabilities and threats to these functions.
7. Calculate the risk for each different business function.
8. Document findings and report them to management.
Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 905-909). McGraw-Hill. Kindle Edition.

QUESTION 524
Which one of the following is NOT one of the outcomes of a vulnerability assessment?

A. Quantative loss assessment
B. Qualitative loss assessment
C. Formal approval of BCP scope and initiation document
D. Defining critical support areas

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: When seeking to determine the security position of an organization, the security professional will eventually turn to a vulnerability assessment to help identify specific areas of weakness that need to be addressed. A vulnerability assessment is the use of various tools and analysis methodologies to determine where a particular system or process may be susceptible to attack or misuse. Most vulnerability assessments concentrate on technical vulnerabilities in systems or applications, but the assessment process is equally as effective when examining physical or administrative business processes.
The vulnerability assessment is often part of a BI
A. It is similar to a Risk Assessment in that there
is a quantitative (financial) section and a qualitative (operational) section. It differs in that i t is smaller than a full risk assessment and is focused on providing information that is used solely for the business continuity plan or disaster recovery plan. A function of a vulnerability assessment is to conduct a loss impact analysis. Because there will be two parts to the assessment, a financial assessment and an operational assessment, it will be necessary to define loss criteria both quantitatively and qualitatively.
Quantitative loss criteria may be defined as follows:
Incurring financial losses from loss of revenue, capital expenditure, or personal liability resolution The additional operational expenses incurred due to the disruptive event Incurring financial loss from resolution of violation of contract agreements Incurring financial loss from resolution of violation of regulatory or compliance requirements Qualitative loss criteria may consist of the following:
The loss of competitive advantage or market share
The loss of public confidence or credibility, or incurring public mbarrassment During the vulnerability assessment, critical support areas must be defined in order to assess the impact of a disruptive event. A critical support area is defined as a business unit or function that must be present to sustain continuity of the business processes, maintain life safety, or avoid public relations embarrassment.
Critical support areas could include the following:
Telecommunications, data communications, or information technology areas Physical infrastructure or plant facilities, transportation services Accounting, payroll, transaction processing, customer service, purchasing The granular elements of these critical support areas will also need to be identified. By granular elements we mean the personnel, resources, and services the critical support areas need to maintain business continuity
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 4628-4632). Auerbach Publications. Kindle Edition. KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Page 277.

QUESTION 525
The scope and focus of the Business continuity plan development depends most on:

A. Directives of Senior Management
B. Business Impact Analysis (BIA)
C. Scope and Plan Initiation
D. Skills of BCP committee

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: SearchStorage.com Definitions mentions "As part of a disaster recovery plan, BIA is likely to identify costs linked to failures, such as loss of cash flow, replacement of equipment, salaries paid to catch up with a backlog of work, loss of profits, and so on. A BIA report quantifies the importance of business components and suggests appropriate fund allocation for measures to protect them. The possibilities of failures are likely to be assessed in terms of their impacts on safety, finances, marketing, legal compliance, and quality assurance. Where possible, impact is expressed monetarily for purposes of comparison. For example, a business may spend three times as much on marketing in the wake of a disaster to rebuild customer confidence."
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Page 278.

QUESTION 526
Which of the following items is NOT a benefit of cold sites?

A. No resource contention with other organisation
B. Quick Recovery
C. A secondary location is available to reconstruct the environment
D. Low Cost

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: A cold site is a permanent location that provide you with your own space that you can move into in case of a disaster or catastrophe. It is one of the cheapest solution available as a rental place but it is also the one that would take the most time to recover. A cold site usuallytakes one to two weeks for recoverey.
Although major disruptions with long-term effects may be rare, they should be accounted for in the contingency plan. The plan should include a trategy to recover and perform system operations at an alternate facility for an extended period. In general, three types of alternate sites are available:
Dedicated site owned or operated by the organization. Also called redundant or alternate sites; Reciprocal agreement or memorandum of agreement with an internal or external entity; and Commercially leased facility.
Regardless of the type of alternate site chosen, the facility must be able to support system operations as defined in the contingency plan. The three alternate site types commonly categorized in terms of their operational readiness are cold sites, warm sites, or hot sites. Other variations or combinations of these can be found, but generally all variations retain similar core features found in one of these three site types.
Progressing from basic to advanced, the sites are described below:
Cold Sites are typically facilities with adequate space and infrastructure (electric power, telecommunications connections, and environmental controls) to support information system recovery activities.
Warm Sites are partially equipped office spaces that contain some or all of the system hardware, software, telecommunications, and power sources.
Hot Sites are facilities appropriately sized to support system requirements and configured with the necessary system hardware, supporting infrastructure, and support personnel. As discussed above, these three alternate site types are the most common. There are also variations, and hybrid mixtures of features from any one of the three. Each organization should evaluate its core requirements in order to establish the most effective solution.

Two examples of variations to the site types are:
Mobile Sites are self-contained, transportable shells custom-fitted with specific telecommunications and system equipment necessary to meet system requirements. Mirrored Sites are fully redundant facilities with automated real-time information mirroring. Mirrored sites are identical to the primary site in all technical respects. There are obvious cost and ready-time differences among the options. In these examples, the mirrored site is the most expensive choice, but it ensures virtually 100 percent availability. Cold sites are the least expensive to maintain, although they may require substantial time to acquire and install necessary equipment. Partially equipped sites, such as warm sites, fall in the middle of the spectrum. In many cases, mobile sites may be delivered to the desired location within 24 hours, but the time necessary for equipment installation and setup can increase this response time. The selection of fixed-site locations should account for the time and mode of transportation necessary to move personnel and/or equipment there. In addition, the fixed site should be in a geographic area that is unlikely to be negatively affected by the same hazard as the organization's primary site.
The following reference(s) were used for this question:
http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf
Exam B

QUESTION 527
Qualitative loss resulting from the business interruption does NOT usually include:

A. Loss of revenue
B. Loss of competitive advantage or market share
C. Loss of public confidence and credibility
D. Loss of market leadership

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: This question is testing your ability to evaluate whether items on the list are Qualitative or Quantitative. All of the items listed were Qualitative except Lost of Revenue which is Quantitative.
Those are mainly two approaches to risk analysis, see a description of each below:
A quantitative risk analysis is used to assign monetary and numeric values to all elements of the risk analysis process. Each element within the analysis (asset value, threat frequency, severity of vulnerability, impact damage, safeguard costs, safeguard effectiveness, uncertainty, and probability items) is quantified and entered into equations to determine total and residual risks. It is more of a scientific or mathematical approach to risk analysis compared to qualitative. A qualitative risk analysis uses a "softer" approach to the data elements of a risk analysis . It does not quantify that data, which means that it does not assign numeric values to the data so that they can be used in equations.
Qualitative and quantitative impact information should be gathered and then properly analyzed and interpreted. The goal is to see exactly how a business will be affected by different threats. The effects can be economical, operational, or both. Upon completion of the data analysis, it should be reviewed with the most knowledgeable people within the company to ensure that the findings are appropriate and that it describes the real risks and impacts the organization faces. This will help flush out any additional data points not originally obtained and will give a fuller understanding of all the possible business impacts.
Loss criteria must be applied to the individual threats that were identified. The criteria may include the following:
Loss in reputation and public confidence
Loss of competitive advantages
Increase in operational expenses
Violations of contract agreements
Violations of legal and regulatory requirements
Delayed income costs
Loss in revenue
Loss in productivity
Reference used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 909). McGraw-Hill.
Kindle Edition.

QUESTION 528
When you update records in multiple locations or you make a copy of the whole database at a remote location as a way to achieve the proper level of fault-tolerance and redundancy, it is knows as?

A. Shadowing
B. Data mirroring
C. Backup
D. Archiving

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Updating records in multiple locations or copying an entire database to a remote location as a means to ensure the appropriate levels of fault-tolerance and redundancy is known as Database shadowing. Shadowing is the technique in which updates are shadowed in multiple locations. It is like copying the entire database on to a remote location. Shadow files are an exact live copy of the original active database, allowing you to maintain live duplicates of your production database, which can be brought into production in the event of a hardware failure. They are used for security reasons: should the original database be damaged or incapacitated by hardware problems, the shadow can immediately take over as the primary database. It is therefore important that shadow files do not run on the same server or at least on the same drive as the primary database files.
The following are incorrect answers:
Data mirroring In data storage, disk mirroring is the replication of logical disk volumes onto separate physical hard disks in real time to ensure continuous availability. It is most commonly used in RAID 1. A mirrored volume is a complete logical representation of separate volume copies.
Backups In computing the phrase backup means to copy files to a second medium (a disk or tape) as a precaution in case the first medium fails. One of the cardinal rules in using computers is back up your files regularly. Backups are useful in recovering information or a system in the event of a disaster, else you may be very sorry :-(
Archiving is the storage of data that is not in continual use for historical purposes. It is the process of copying files to a long-term storage medium for backup.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 27614-27626). Auerbach Publications. Kindle Edition.
http://en.wikipedia.org/wiki/Disk_mirroring
http://www.webopedia.com/TERM/A/archive.html
http://ibexpert.net/ibe/index.php?n=Doc.DatabaseShadow

QUESTION 529
Recovery Site Strategies for the technology environment depend on how much downtime an organization can tolerate before the recovery must be completed. What would you call a strategy where the alternate site is internal, standby ready, with all the technology and equipment necessary to run the applications?

A. External Hot site
B. Warm Site
C. Internal Hot Site
D. Dual Data Center

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Internal Hot Site--This site is standby ready with all the technology and equipment necessary to run the applications positioned there. The planner will be able to effectively restart an application in a hot site recovery without having to perform any bare metal recovery of servers. If this is an internal solution, then often

the organization will run non-time sensitive processes there such as development or test environments, which will be pushed aside for recovery of production when needed. When employing this strategy, it is important that the two environments be kept as close to identical as possible to avoid problems with O/S levels, hardware differences, capacity differences, etc., from preventing or delaying recovery. Recovery Site Strategies Depending on how much downtime an organization has before the technology recovery must be complete, recovery strategies selected for the technology environment could be any one of the following:
Dual Data Center--This strategy is employed for applications, which cannot accept any downtime without negatively impacting the organization. The applications are split between two geographically dispersed data centers and either load balanced between the two centers or hot swapped between the two centers. The surviving data center must have enough head room to carry the full production load in either case.
External Hot Site--This strategy has equipment on the floor waiting, but the environment must be rebuilt for the recovery. These are services contracted through a recovery service provider. Again, it is important that the two environments be kept as close to identical as possible to avoid problems with O/S levels, hardware differences, capacity differences, etc., from preventing or delaying recovery. Hot site vendors tend to have the most commonly used hardware and software products to attract the largest number of customers to utilize the site. Unique equipment or software would generally need to be provided by the organization either at time of disaster or stored there ahead of time.
Warm Site--A leased or rented facility that is usually partially configured with some equipment, but not the actual computers. It will generally have all the cooling, cabling, and networks in place to accommodate the recovery but the actual servers, mainframe, etc., equipment are delivered to the site at time of disaster.
Cold Site--A cold site is a shell or empty data center space with no technology on the floor. All technology must be purchased or acquired at the time of disaster.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 21265-21291). Auerbach Publications. Kindle Edition.

QUESTION 530
What is the most correct choice below when talking about the steps to resume normal operation at the primary site after the green light has been given by the salvage team?

A. The most critical operations are moved from alternate site to primary site before others
B. Operation may be carried by a completely different team than disaster recovery team
C. The least critical functions should be moved back first
D. You moves items back in the same order as the categories document in your plan or exactly in the same order as you did on your way to the alternate site

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: It's interesting to note that the steps to resume normal processing operations will be different than the steps of the recovery plan; that is, the least critical work should be broughtback first to the primary site.
The most important point above in the steps would be to move the least critical items or resources back to the primary site first. This way you can ensure that the site was really well prepared and that all is working fine.
Before that first step would be done, you would get the green light from the salvage team that it is fine to move back to the primary site. The first step after getting the green light would be to move the least critical elements first.
As stated in the Shon Harris book:
The least critical functions should be moved back first, so if there are issues in network configurations or connectivity, or important steps were not carried out, the critical operations of the company are not negatively affected. Why go through the trouble of moving the most critical systems and operations to a safe and stable site, only to return it to a main site that is untested? Let the less critical departments act as the canary. If they survive, then move over the more critical components of the company.
When it is time for the company to move back into its original site or a new site, the company enters the reconstitution phase. A company is not out of an emergency state until it is back in operation at the original primary site or a new site that was constructed to replace the primary site, because the company is always vulnerable while operating in a backup facility. Many logistical issues need to be considered as to when a company must return from the alternate site to the original site. The following lists a few of these issues:

Ensuring the safety of employees
Ensuring an adequate environment is provided (power, facility infrastructure, water, HVAC) Ensuring that the necessary equipment and supplies are present and in working order Ensuring proper communications and connectivity methods are working Properly testing the new environment
Once the coordinator, management, and salvage team sign off on the readiness of the facility, the salvage team should carry out the following steps:
Back up data from the alternate site and restore it within the new facility.
Carefully terminate contingency operations.
Securely transport equipment and personnel to the new facility.
All other choices are not the correct answer.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Location 19389).
McGraw-Hill. Kindle Edition.
and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Page 290.

QUESTION 531
What would be the Annualized Rate of Occurrence (ARO) of the threat "user input error", in the case where a company employs 100 data entry clerks and every one of them makes one input error each month?

A. 100
B. 120
C. 1
D. 1200

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: If every one of the 100 clerks makes 1 error 12 times per year, it makes a total of 1200 errors. The Annnualized Rate of Occurence (ARO) is a value that represents the estimated frequency in which a threat is expected to occur. The range can be from 0.0 to a large number. Having an average of 1200 errors per year means an ARO of 1200

QUESTION 532
How is Annualized Loss Expectancy (ALE) derived from a threat?

A. ARO x (SLE - EF)
B. SLE x ARO
C. SLE/EF
D. AV x EF

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Three steps are undertaken in a quantitative risk assessment:
Initial management approval
Construction of a risk assessment team, and
The review of information currently available within the organization. There are a few formulas that you MUST understand for the exam. See them below:
SLE (Single Loss Expectancy)
Single loss expectancy (SLE) must be calculated to provide an estimate of loss. SLE is defined as the difference between the original value and the remaining value of an asset after a single exploit. The formula for calculating SLE is as follows: SLE = asset value (in $) × exposure factor (loss due to successful threat exploit, as a %)

Losses can include lack of availability of data assets due to data loss, theft, alteration, or denial of service (perhaps due to business continuity or security issues).
ALE (Annualized Loss Expectancy)
Next, the organization would calculate the annualized rate of occurrence (ARO). This is done to provide an accurate calculation of annualized loss expectancy (ALE). ARO is an estimate of how often a threat will be successful in exploiting a vulnerability over the period of a year.
When this is completed, the organization calculates the annualized loss expectancy (ALE). The ALE is a product of the yearly estimate for the exploit (ARO) and the loss in value of an asset after an SLE.
The calculation follows ALE = SLE x ARO
Note that this calculation can be adjusted for geographical distances using the local annual frequency estimate (LAFE) or the standard annual frequency estimate (SAFE). Given that there is now a value for SLE, it is possible to determine what the organization should spend, if anything, to apply a countermeasure for the risk in question.
Remember that no countermeasure should be greater in cost than the risk it mitigates, transfers, or avoids. Countermeasure cost per year is easy and straightforward to calculate. It is simply the cost of the countermeasure divided by the years of its life (i.e., use within the organization). Finally, the organization is able to compare the cost of the risk versus the cost of the countermeasure and make some objective decisions regarding its countermeasure selection.
The following were incorrect answers:
All of the other choices were incorrect.
The following reference(s) were used for this quesiton:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 10048-10069). Auerbach Publications. Kindle Edition.

QUESTION 533
What does "residual risk" mean?

A. The security risk that remains after controls have been implemented
B. Weakness of an assets which can be exploited by a threat
C. Risk that remains after risk assessment has has been performed
D. A security risk intrinsic to an asset being audited, where no mitigation has taken place.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Residual risk is "The security risk that remains after controls have been implemented" ISO/IEC TR 13335-1 Guidelines for the Management of IT Security (GMITS), Part
1: Concepts and Models for IT Security, 1996. "Weakness of an assets which can be exploited by a threat" is vulnerability. "The result of unwanted incident" is impact. Risk that remains after risk analysis has been performed is a distracter.
Risk can never be eliminated nor avoided, but it can be mitigated, transferred or accpeted. Even after applying a countermeasure like for example putiing up an Antivirus. But still it is not 100% that systems will be protected by antivirus.

QUESTION 534
Business Continuity and Disaster Recovery Planning (Primarily) addresses the:

A. Availability of the CIA triad
B. Confidentiality of the CIA triad
C. Integrity of the CIA triad
D. Availability, Confidentiality and Integrity of the CIA triad

Correct Answer: A
Explanation

Explanation/Reference:

Explanation: The Information Technology (IT) department plays a very important role in identifying and protecting the company's internal and external information dependencies. Also, the information technology elements of the BCP should address several vital issue, including:
Ensuring that the company employs sufficient physical security mechanisms to preserve vital network and hardware components. including file and print servers. Ensuring that the organization uses sufficient logical security methodologies (authentication, authorization, etc.) for sensitive data.
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, page 279.

QUESTION 535
What is called an event or activity that has the potential to cause harm to the information systems or networks?

A. Vulnerability
B. Threat agent
C. Weakness
D. Threat

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 16, 32.

QUESTION 536
A weakness or lack of a safeguard, which may be exploited by a threat, causing harm to the information systems or networks is called a ?

A. Vulnerability
B. Risk
C. Threat
D. Overflow

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The
Answer: Vulnerability; Vulnerability is a weakness or lack of a safeguard, which may be exploited by a threat, causing harm to the information systems or networks. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 16, 32.

QUESTION 537
What is called the probability that a threat to an information system will materialize?

A. Threat
B. Risk
C. Vulnerability
D. Hole

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The

Answer: Risk: The potential for harm or loss to an information system or network; the probability that a threat will materialize. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 16, 32.

QUESTION 538
Risk mitigation and risk reduction controls for providing information security are classified within three main categories, which of the following are being used?

A. preventive, corrective, and administrative

B. detective, corrective, and physical

C. Physical, technical, and administrative

D. Administrative, operational, and logical

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Security is generally defined as the freedom from danger or as the condition of safety. Computer security, specifically, is the protection of data in a system against unauthorized disclosure, modification, or destruction and protection of the computer system itself against unauthorized use, modification, or denial of service. Because certain computer security controls inhibit productivity, security is typically a compromise toward which security practitioners, system users, and system operations and administrative personnel work to achieve a satisfactory balance between security and productivity.
Controls for providing information security can be physical, technical, or administrative. These three categories of controls can be further classified as either preventive or detective. Preventive controls attempt to avoid the occurrence of unwanted events, whereas detective controls attempt to identify unwanted events after they have occurred. Preventive controls inhibit the free use of computing resources and therefore can be applied only to the degree that the users are willing to accept. Effective security awareness programs can help increase users' level of tolerance for preventive controls by helping them understand how such controls enable them to trust their computing systems. Common detective controls include audit trails, intrusion detection methods, and checksums.
Three other types of controls supplement preventive and detective controls. They are usually described as deterrent, corrective, and recovery.
Deterrent controls are intended to discourage individuals from intentionally violating information security policies or procedures. These usually take the form of constraints that make it difficult or undesirable to perform unauthorized activities or threats of consequences that influence a potential intruder to not violate security (e.g., threats ranging from embarrassment to severe punishment).
Corrective controls either remedy the circumstances that allowed the unauthorized activity or return conditions to what they were before the violation. Execution of corrective controls could result in changes to existing physical, technical, and administrative controls. Recovery controls restore lost computing resources or capabilities and help the organization recover monetary losses caused by a security violation. Deterrent, corrective, and recovery controls are considered to be special cases within the major categories of physical, technical, and administrative controls; they do not clearly belong in either preventive or detective categories. For example, it could be argued that deterrence is a form of prevention because it can cause an intruder to turn away; however, deterrence also involves detecting violations, which may be what the intruder fears most. Corrective controls, on the other hand, are not preventive or detective, but they are clearly linked with technical controls when antiviral software eradicates a virus or with administrative controls when backup procedures enable restoring a damaged data base. Finally, recovery controls are neither preventive nor detective but are included in administrative controls as disaster recovery or contingency plans.
Reference(s) used for this question
Handbook of Information Security Management, Hal Tipton

QUESTION 539
In the course of responding to and handling an incident, you work on determining the root cause of the incident. In which step are you in?

A. Recovery

B. Containment

C. Triage
D. Analysis and tracking

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: In this step, your main objective is to examine and analyze what has occurred and focus on determining the root cause of the incident.
Recovery is incorrect as recovery is about resuming operations or bringing affected systems back into production
Containment is incorrect as containment is about reducing the potential impact of an incident. Triage is incorrect as triage is about determining the seriousness of the incident and filtering out false positives
Official Guide to the CISSP CBK, pages 700-704

QUESTION 540
Which of the following assertions is NOT true about pattern matching and anomaly detection in intrusion detection?

A. Anomaly detection tends to produce more data
B. A pattern matching IDS can only identify known attacks
C. Stateful matching scans for attack signatures by analyzing individual packets instead of traffic streams
D. An anomaly-based engine develops baselines of normal traffic activity and throughput, and alerts on deviations from these baselines

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: This is wrong which makes this the correct choice. This statement is not true as stateful matching scans for attack signatures by analyzing traffic streams rather than individual packets. Stateful matching intrusion detection takes pattern matching to the next level. As networks become faster there is an emerging need for security analysis techniques that can keep up with the increased network throughput. Existing network-based intrusion detection sensors can barely keep up with bandwidths of a few hundred Mbps. Analysis tools that can deal with higher throughput are unable to maintain state between different steps of an attack or they are limited to the analysis of packet headers.
The following answers are all incorrect:
Anomaly detection tends to produce more data is true as an anomaly-based IDS produces a lot of data as any activity outside of expected behavior is recorded. A pattern matching IDS can only identify known attacks is true as a pattern matching IDS works by comparing traffic streams against signatures. These signatures are created for known attacks. An anomaly-based engine develops baselines of normal traffic activity and throughput, and alerts on deviations from these baselines is true as the assertion is a characteristic of a statistical anomaly-based IDS.
Official guide to the CISSP CBK. Pages 198 to 201
http://cs.ucsb.edu/~vigna/publications/2003_vigna_robertson_kher_kemmerer_ACSAC03.pdf

QUESTION 541
The IP header contains a protocol field. If this field contains the value of 51, what type of data is contained within the ip datagram?

A. Transmission Control Protocol (TCP)
B. Authentication Header (AH)
C. User datagram protocol (UDP)
D. Internet Control Message Protocol (ICMP)

Correct Answer: B

Explanation

Explanation/Reference:
Explanation: TCP has the value of 6
UDP has the value of 17
ICMP has the value of 1
SANS http://www.sans.org/resources/tcpip.pdf?ref=3871

QUESTION 542
Which of the following is NOT a correct notation for an IPv6 address?

A. 2001:0db8:0:0:0:0:1428:57ab
B. ABCD:EF01:2345:6789:ABCD:EF01:2345:6789
C. ::1
D. 2001:DB8::8:800::417A

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: This is not a correct notation for an IPv6 address because the the "::" can only appear once in an address. The use of "::" is a shortcut notation that indicates one or more groups of 16 bits of zeros.
1 is the loopback address using the special notation
IP Version 6 Addressing Architecture
http://tools.ietf.org/html/rfc4291#section-2.1

QUESTION 543
Another example of Computer Incident Response Team (CIRT) activities is:

A. Management of the netware logs, including collection, retention, review, and analysis of data
B. Management of the network logs, including collection and analysis of data
C. Management of the network logs, including review and analysis of data
D. Management of the network logs, including collection, retention, review, and analysis of data

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Additional examples of CIRT activities are:
Management of the network logs, including collection, retention, review, and analysis of data Management of the resolution of an incident, management of the remediation of a vulnerability, and post-event reporting to the appropriate parties.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 64.

QUESTION 544
Which of the following backup methods makes a complete backup of every file on the server every time it is run?

A. full backup method.
B. incremental backup method.
C. differential backup method.
D. tape backup method.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The Full Backup Method makes a complete backup of every file on the server every time it is run.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 69.

QUESTION 545
Which of the following backup methods is primarily run when time and tape space permits, and is used for the system archive or baselined tape sets?

A. full backup method.
B. incremental backup method.
C. differential backup method.
D. tape backup method.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The Full Backup Method is primarily run when time and tape space permits, and is used for the system archive or baselined tape sets.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 69.

QUESTION 546
Which backup method usually resets the archive bit on the files after they have been backed up?

A. Incremental backup method.
B. Differential backup method.
C. Partial backup method.
D. Tape backup method.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The incremental backup method usually resets the archive bit on the files after they have been backed up.
An Incremental Backup will backup all the files that have changed since the last Full Backup (the first time it is run after a full backup was previously completed) or after an Incremental Backup (for the second backup and subsequent backups) and sets the archive bit to 0. This type of backup take less time during the backup phase but it will take more time to restore.
The other answers are all incorrect choices.
The following backup types also exists:
Full Backup - All data are backed up. The archive bit is cleared, which means that it is set to 0. Differential Backup - Backup the files that have been modified since the last Full Backup. The archive bit does not change. Take more time while the backup phase is performed and take less time to restore.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 69.

QUESTION 547
Which backup method is used if backup time is critical and tape space is at an extreme premium?

A. Incremental backup method.
B. Differential backup method.

C. Full backup method.

D. Tape backup method.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Full Backup/Archival Backup - Complete/Full backup of every selected file on the system regardless of whether it has been backup recently.. This is the slowest of the backup methods since it backups all the data. It's however the fastest for restoring data. Incremental Backup - Any backup in which only the files that have been modified since last full back up are backed up. The archive attribute should be updated while backing up only modified files, which indicates that the file has been backed up. This is the fastest of the backup methods, but the slowest of the restore methods.
Differential Backup - The backup of all data files that have been modified since the last incremental backup or archival/full backup. Uses the archive bit to determine what files have changed since last incremental backup or full backup. The files grows each day until the next full backup is performed clearing the archive attributes. This enables the user to restore all files changed since the last full backup in one pass. This is a more neutral method of backing up data since it's not faster nor slower than the other two
Easy Way To Remember each of the backup type properties:
Backup Speed Restore Speed
Full 3 1
Differential 2 2
Incremental 1 3
Legend: 1 = Fastest 2 = Faster 3 = Slowest
Source:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 69.
and
http://www.proprofs.com/mwiki/index.php/Full_Backup,_Incremental_%26_Differential_Backup

QUESTION 548
Which backup method copies only files that have changed since the last full backup, but does not clear the archive bit?

A. Differential backup method.

B. Full backup method.

C. Incremental backup method.

D. Tape backup method.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: One of the key item to understand regarding backup is the archive bit. The archive bit is used to determine what files have been backuped already. The archive bit is set if a file is modified or a new file is created, this indicates to the backup program that it has to be saved on the next backup. When a full backup is performed the archive bit will be cleared indicating that the files were backup. This allows backup programs to do an incremental or differential backup that only backs up the changes to the filesystem since the last time the bit was cleared Full Backup (or Reference Backup)
A Full backup will backup all the files and folders on the drive every time you run the full backup. The archive bit is cleared on all files indicating they were all backuped.
Advantages:
All files from the selected drives and folders are backed up to one backup set. In the event you need to restore files, they are easily restored from the single backup set.
Disadvantages:
A full backup is more time consuming than other backup options. Full backups require more disk, tape, or network drive space.
Incremental Backup

An incremental backup provides a backup of files that have changed or are new since the last incremental backup.
For the first incremental backup, all files in the file set are backed up (just as in a full backup). If you use the same file set to perform a incremental backup later, only the files that have changed are backed up. If you use the same file set for a third backup, only the files that have changed since the second backup are backed up, and so on.
Incremental backup will clear the archive bit.
Advantages:
Backup time is faster than full backups.
Incremental backups require less disk, tape, or network drive space. You can keep several versions of the same files on different backup sets.
Disadvantages:
In order to restore all the files, you must have all of the incremental backups available. It may take longer to restore a specific file since you must search more than one backup set to find the latest version of a file.
Differential Backup
A differential backup provides a backup of files that have changed since a full backup was performed. A differential backup typically saves only the files that are different or new since the last full backup. Together, a full backup and a differential backup include all the files on your computer, changed and unchanged.
Differential backup do not clear the archive bits.
Advantages:
Differential backups require even less disk, tape, or network drive space than incremental backups.
Backup time is faster than full or incremental backups.
Disadvantages:
Restoring all your files may take considerably longer since you may have to restore both the last differential and full backup.
Restoring an individual file may take longer since you have to locate the file on either the differential or full backup.
For more info see: http://support.microsoft.com/kb/136621 Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 69.

QUESTION 549
Which backup method is additive because the time and tape space required for each night's backup grows during the week as it copies the day's changed files and the previous days' changed files up to the last full backup?

A. differential backup method
B. full backup method
C. incremental backup method
D. tape backup method.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The Differential Backup Method is additive because the time and tape space required for each night's backup grows during the week as it copies the day's changed files and the previous days' changed files up to the last full backup.
Archive Bits
Unless you've done a lot of backups in your time you've probably never heard of an Archive Bit. An archive bit is, essentially, a tag that is attached to every file. In actuality, it is a binary digit that is set on or off in the file, but that's crummy technical jargon that doesn't really tell us anything. For the sake of our discussion, just think of it as the flag on a mail box. If the flag is up, it means the file has been changed. If it's down, then the file is unchanged. Archive bits let the backup software know what needs to be backed up. The differential and incremental backup types rely on the archive bit to direct them.
Backup Types
Full or Normal
The "Full" or "normal" backup type is the most standard. This is the backup type that you would use if you

wanted to backup every file in a given folder or drive. It backs up everything you direct it to regardless of what the archive bit says. It also resets all archive bits (puts the flags down). Most backup software, including the built-in Windows backup software, lets you select down to the individual file that you want backed up. You can also choose to backup things like the "system state".
Incremental
When you schedule an incremental backup, you are in essence instructing the software to only backup files that have been changed, or files that have their flag up. After the incremental backup of that file has occured, that flag will go back down. If you perform a normal backup on Monday, then an incremental backup on Wednesday, the only files that will be backed up are those that have changed since Monday. If on Thursday someone deletes a file by accident, in order to get it back you will have to restore the full backup from Monday, followed by the Incremental backup from Wednesday.
Differential
Differential backups are similar to incremental backups in that they only backup files with their archive bit, or flag, up. However, when a differential backup occurs it does not reset those archive bits which means, if the following day, another differential backup occurs, it will back up that file again regardless of whether that file has been changed or not. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 69. And: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 9: Disaster Recovery and Business continuity (pages 617-619). And: http://www.brighthub.com/computing/windows-platform/articles/24531.aspx

QUESTION 550
Which of the following backup method must be made regardless of whether Differential or Incremental methods are used?

A. Full Backup Method.
B. Incremental backup method.
C. Supplemental backup method.
D. Tape backup method.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: A Full Backup must be made regardless of whether Differential or Incremental methods are used. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 69. And: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 9: Disaster Recovery and Business continuity (pages 617-619).

QUESTION 551
Which of the following tape formats can be used to backup data systems in addition to its original intended audio uses?

A. Digital Video Tape (DVT).
B. Digital Analog Tape (DAT).
C. Digital Voice Tape (DVT).
D. Digital Audio Tape (DAT).

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Digital Audio Tape (DAT) can be used to backup data systems in addition to its original intended audio uses.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 70.

QUESTION 552
Which of the following is a large hardware/software backup system that uses the RAID technology?

A. Tape Array.
B. Scale Array.
C. Crimson Array
D. Table Array.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: A Tape Array is a large hardware/software backup system based on the RAID technology.
There is a misconception that RAID can only be used with Disks. All large storage vendor from HP, to EMC, to Compaq have Tape Array based on RAID technology they offer.
This is a VERY common type of storage at an affordable price as well. So RAID is not exclusively for DISKS.
Often time this is referred to as Tape Librairies or simply RAIT.
RAIT (redundant array of independent tapes) is similar to RAID, but uses tape drives instead of disk drives.
Tape storage is the lowest-cost option for very large amounts of data, but is very slow compared to disk storage. As in RAID 1 striping, in RAIT, data are striped in parallel to multiple tape drives, with or without a redundant parity drive. This provides the high capacity at low cost typical of tape storage, with higher-than-usual tape data transfer rates and optional data integrity.

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 70.
and
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 1271). McGraw-Hill.
Kindle Edition.

QUESTION 553
This type of backup management provides a continuous on-line backup by using optical or tape "jukeboxes," similar to WORMs (Write Once, Read Many):

A. Hierarchical Storage Management (HSM).
B. Hierarchical Resource Management (HRM).
C. Hierarchical Access Management (HAM).
D. Hierarchical Instance Management (HIM).

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Hierarchical Storage Management (HSM) provides a continuous on-line backup by using optical or tape "jukeboxes," similar to WORMs.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 71.

QUESTION 554
Hierarchical Storage Management (HSM) is commonly employed in:

A. very large data retrieval systems
B. very small data retrieval systems
C. shorter data retrieval systems
D. most data retrieval systems

Correct Answer: A

Explanation

Explanation/Reference:
Explanation: Hierarchical Storage Management (HSM) is commonly employed in very large data retrieval systems.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 71.

QUESTION 555
Physically securing backup tapes from unauthorized access is obviously a security concern and is considered a function of the:

A. Operations Security Domain.
B. Operations Security Domain Analysis.
C. Telecommunications and Network Security Domain.
D. Business Continuity Planning and Disater Recovery Planning.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Physically securing the tapes from unauthorized access is obviously a security concern and is considered a function of the Operations Security Domain. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 71.

QUESTION 556
What is the MOST critical piece to disaster recovery and continuity planning?

A. Security policy
B. Management support
C. Availability of backup information processing facilities
D. Staff training

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The keyword is ' MOST CRITICAL ' and the correct answer is ' Management Support ' as the management must be convinced of its necessity and that's why a business case must be made. The decision of how a company should recover from any disaster is purely a business decision and should be treated as so.
The other answers are incorrect because :
Security policy is incorrect as it is not the MOST CRITICAL piece. Availability of backup information processing facilities is incorrect as this comes once the organization has BCP Plans in place and for a BCP Plan , management support must be there. Staff training comes after the plans are in place with the support from management. Reference : Shon Harris , AIO v3 , Chapter-9: Business Continuity Planning , Page : 697.

QUESTION 557
During the testing of the business continuity plan (BCP), which of the following methods of results analysis provides the BEST assurance that the plan is workable?

A. Measurement of accuracy
B. Elapsed time for completion of critical tasks
C. Quantitatively measuring the results of the test
D. Evaluation of the observed test results

Correct Answer: C

Explanation

Explanation/Reference:
Explanation: It is important to have ways to measure the success of the plan and tests against the stated objectives. Therefore, results must be quantitatively gauged as opposed to an evaluation based only on observation. Quantitatively measuring the results of the test involves a generic statement measuring all the activities performed during BCP, which gives the best assurance of an effective plan. Although choices A and B are also quantitative, they relate to specific areas, or an analysis of results from one viewpoint, namely the accuracy of the results and the elapsed time.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 5: Disaster Recovery and Business Continuity (page 269).

QUESTION 558
Which of the following statements regarding an off-site information processing facility is TRUE?

A. It should have the same amount of physical access restrictions as the primary processing site.
B. It should be located in proximity to the originating site so that it can quickly be made operational.
C. It should be easily identified from the outside so in the event of an emergency it can be easily found.
D. Need not have the same level of environmental monitoring as the originating site since this would be cost prohibitive.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: It is very important that the offsite has the same restrictions in order to avoide misuse.
The following answers are incorrect because:
It should be located in proximity to the originating site so that it can quickly be made operational is incorrect as the offsite is also subject to the same disaster as of the primary site. It should be easily identified from the outside so in the event of an emergency it can be easily found is also incorrect as it should not be easily identified to prevent intentional sabotage. Need not have the same level of environmental monitoring as the originating site since this would be cost prohibitive is also incorrect as it should be like its primary site.
Reference : Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 5: Disaster Recovery and Business Continuity (page 265).

QUESTION 559
What is the PRIMARY goal of incident handling?

A. Successfully retrieve all evidence that can be used to prosecute
B. Improve the company's ability to be prepared for threats and disasters
C. Improve the company's disaster recovery plan
D. Contain and repair any damage caused by an event.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: This is the PRIMARY goal of an incident handling process.
The other answers are incorrect because :
Successfully retrieve all evidence that can be used to prosecute is more often used in identifying weaknesses than in prosecuting.
Improve the company's ability to be prepared for threats and disasters is more appropriate for a disaster recovery plan.
Improve the company's disaster recovery plan is also more appropriate for disaster recovery plan. Reference : Shon Harris AIO v3 , Chapter - 10 : Law, Investigation, and Ethics , Page : 727-728

QUESTION 560

Which of the following outlined how senior management are responsible for the computer and information security decisions that they make and what actually took place within their organizations?

A. The Computer Security Act of 1987.
B. The Federal Sentencing Guidelines of 1991.
C. The Economic Espionage Act of 1996.
D. The Computer Fraud and Abuse Act of 1986.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: In 1991, U.S. Federal Sentencing Guidelines were developed to provide judges with courses of action in dealing with white collar crimes. These guidelines provided ways that companies and law enforcement should prevent, detect and report computer crimes. It also outlined how senior management are responsible for the computer and information security decisions that they make and what actually took place within their organizations.

QUESTION 561
What is the PRIMARY reason to maintain the chain of custody on evidence that has been collected?

A. To ensure that no evidence is lost.
B. To ensure that all possible evidence is gathered.
C. To ensure that it will be admissible in court
D. To ensure that incidents were handled with due care and due diligence.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: This is the PRIMARY reason for the chain of custody of evidence. Evidence must be controlled every step of the way. If it is not, the evidence can be tampered with and ruled inadmissable. The Chain of Custody will include a detailed record of:
Who obtained the evidence
What was the evidence
Where and when the evidence was obtained
Who secured the evidence
Who had control or possession of the evidence
The following answers are incorrect because :
To ensure that no evidence is lost is incorrect as it is not the PRIMARY reason. To ensure that all possible evidence is gathered is also incorrect as it is not the PRIMARY reason. To ensure that incidents were handled with due care and due diligence is also incorrect as it is also not the PRIMARY reason.
The chain of custody is a history that shows how evidence was collected, analyzed, transported, and preserved in order to establish that it is sufficiently trustworthy to be presented as evidence in court. Because electronic evidence can be easily modified, a clearly defined chain of custody demonstrates that the evidence is trustworthy which would make it admissible in court. Reference : Shon Harris AIO v3 , Chapter-10: Law, Investigation, and Ethics , Page : 727

QUESTION 562
Which of the following would BEST be defined as an absence or weakness of safeguard that could be exploited?

A. A threat
B. A vulnerability
C. A risk
D. An exposure

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: It is a software , hardware or procedural weakness that may provide an attacker the open door he is looking for to enter a computer or network and have unauthorized access to resources within the environment. A vulnerability characterizes the absence or weakness of a safeguard that could be exploited. This vulnerability may be a service running on a server, unpatched applications or operating system software etc.
The following answers are incorrect because:
Threat: A threat is defined as a potential danger to information or systems. The threat is someone or something will identify a specific vulnerability and use it against the company or individual. The entity that takes advantage of a vulnerability is referred to as a 'Threat Agent'. A threat agent could be an intruder accessing the network through a port on the firewall , a process accessing data that violates the security policy.
Risk:A risk is the likelihood of a threat agent taking advantage of a vulnerability and the corresponding business impact. If a firewall has several ports open , there is a higher likelihood that an intruder will use one to access the network in an unauthorized method. Exposure: An exposure is an instance of being exposed to losses from a threat agent.

SHON HARRIS , ALL IN ONE THIRD EDITION : Chapter 3 : Security Management Practices , Pages: 57-59

QUESTION 563
Which of the following could be BEST defined as the likelihood of a threat agent taking advantage of a vulnerability?

A. A risk
B. A residual risk
C. An exposure
D. A countermeasure

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Risk is the likelihood of a threat agent taking advantage of a vulnerability and the corresponding business impact. If a firewall has several ports open , there is a higher likelihood that an intruder will use one to access the network in an unauthorized method.
The following answers are incorrect :
Residual Risk is very different from the notion of total risk. Residual Risk would be the risks that still exists after countermeasures have been implemented. Total risk is the amount of risk a company faces if it chooses not to implement any type of safeguard. Exposure: An exposure is an instance of being exposed to losses from a threat agent. Countermeasure: A countermeasure or a safeguard is put in place to mitigate the potential risk. Examples of countermeasures include strong password management , a security guard.
REFERENCES : SHON HARRIS ALL IN ONE 3rd EDITION
Chapter - 3: Security Management Practices , Pages : 57-59

QUESTION 564
Which approach to a security program ensures people responsible for protecting the company's assets are DRIVING the program?

A. The Delphi approach
B. The top-down approach
C. The bottom-up approach
D. The technology approach

Correct Answer: B

Explanation

Explanation/Reference:
Explanation: A security program should use a top-down approach, meaning that the initiation, support, and direction come from top management; work their way through middle management; and then reach staff members.
In contrast, a bottom-up approach refers to a situation in which staff members (usually IT) try to develop a security program without getting proper management support and direction. A bottomup approach is commonly less effective, not broad enough to address all security risks, and doomed to fail.
A top-down approach makes sure the people actually responsible for protecting the company's assets (senior management) are driving the program.
The following are incorrect answers:
The Delphi approach is incorrect as this is for a brainstorming technique. The bottom-up approach is also incorrect as this approach would be if the IT department tried to develop a security program without proper support from upper management. The technology approach is also incorrect as it does not fit into the category of best answer.
Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 63). McGraw-Hill. Kindle Edition.

QUESTION 565
Which of the following is NOT a part of a risk analysis?

A. Identify risks
B. Quantify the impact of potential threats
C. Provide an economic balance between the impact of the risk and the cost of the associated countermeasure
D. Choose the best countermeasure

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: This step is not a part of RISK ANALYSIS. A risk analysis has three main goals: identify risks, quantify the impact of potential threats, and provide an economic balance between the impact of the risk and the cost of the associated countermeasure. Choosing the best countermeasure is not part of the risk analysis.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 3: Security Management Practices (page 73).
HARRIS, Shon, Mike Meyers' CISSP(R) Certification Passport, 2002, McGraw-Hill, page 12.

QUESTION 566
How should a risk be HANDLED when the cost of the countermeasure OUTWEIGHS the cost of the risk?

A. Reject the risk
B. Perform another risk analysis
C. Accept the risk
D. Reduce the risk

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Which means the company understands the level of risk it is faced.
The following answers are incorrect because :
Reject the risk is incorrect as it means ignoring the risk which is dangerous. Perform another risk analysis is also incorrect as the existing risk analysis has already shown the results.
Reduce the risk is incorrect is applicable after implementing the countermeasures. Reference : Shon Harris AIO v3 , Chapter-3: Security Management Practices , Page : 39

QUESTION 567
What would BEST define risk management?

A. The process of eliminating the risk
B. The process of assessing the risks
C. The process of reducing risk to an acceptable level
D. The process of transferring risk

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: This is the basic process of risk management. Risk is the possibility of damage happening and the ramifications of such damage should it occur. Information risk management (IRM) is the process of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain that level. There is no such thing as a 100 percent secure environment. Every environment has vulnerabilities and threats to a certain degree.
The skill is in identifying these threats, assessing the probability of them actually occurring and the damage they could cause, and then taking the right steps to reduce the overall level of risk in the environment to what the organization identifies as acceptable. Proper risk management requires a strong commitment from senior management, a documented process that supports the organization's mission, an information risk management (IRM) policy and a delegated IRM team. Once you've identified your company's acceptable level of risk, you need to develop an information risk management policy. The IRM policy should be a subset of the organization's overall risk management policy (risks to a company include more than just information security issues) and should be mapped to the organizational security policies, which lay out the acceptable risk and the role of security as a whole in the organization. The IRM policy is focused on risk management while the security policy is very high-level and addresses all aspects of security. The IRM policy should address the following items:
Objectives of IRM team
Level of risk the company will accept and what is considered an acceptable risk (as defined in the previous article)
Formal processes of risk identification
Connection between the IRM policy and the organization's strategic planning processes Responsibilities that fall under IRM and the roles that are to fulfill them Mapping of risk to internal controls
Approach for changing staff behaviors and resource allocation in response to risk analysis Mapping of risks to performance targets and budgets
Key indicators to monitor the effectiveness of controls Shon Harris provides a 10,000-foot view of the risk management process below:
A big question that companies have to deal with is, "What is enough security?" This can be restated as, "What is our acceptable risk level?" These two questions have an inverse relationship. You can't know what constitutes enough security unless you know your necessary baseline risk level.
To set an enterprise-wide acceptable risk level for a company, a few things need to be investigated and understood. A company must understand its federal and state legal requirements, its regulatory requirements, its business drivers and objectives, and it must carry out a risk and threat analysis. (I will dig deeper into formalized risk analysis processes in a later article, but for now we will take a broad approach.) The result of these findings is then used to define the company's acceptable risk level, which is then outlined in security policies, standards, guidelines and procedures.
Although there are different methodologies for enterprise risk management, the core components of any risk analysis is made up of the following:
Identify company assets
Assign a value to each asset
Identify each asset's vulnerabilities and associated threats Calculate the risk for the identified assets
Once these steps are finished, then the risk analysis team can identify the necessary countermeasures to mitigate the calculated risks, carry out cost/benefit analysis for these countermeasures and report to senior management their findings. When we look at information security, there are several types of risk a corporation needs to be aware of and address properly. The following items touch on the major categories:
Physical damage Fire, water, vandalism, power loss, and natural disasters Human interaction Accidental or

intentional action or inaction that can disrupt productivity Equipment malfunction Failure of systems and peripheral devices Inside and outside attacks Hacking, cracking, and attacking Misuse of data Sharing trade secrets, fraud, espionage, and theft Loss of data Intentional or unintentional loss of information through destructive means Application error Computation errors, input errors, and buffer overflows The following answers are incorrect:
The process of eliminating the risk is not the best answer as risk cannot be totally eliminated. The process of assessing the risks is also not the best answer. The process of transferring risk is also not the best answer and is one of the ways of handling a risk after a risk analysis has been performed.

Shon Harris , AIO v3 , Chapter 3: Security Management Practices , Page: 66-68 and
http://searchsecurity.techtarget.com/tip/Understanding-risk

QUESTION 568
What is the highest amount a company should spend annually on countermeasures for protecting an asset valued at $1,000,000 from a threat that has an annualized rate of occurrence (ARO) of once every five years and an exposure factor (EF) of 30%?

A. $300,000
B. $150,000
C. $60,000
D. $1,500

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The cost of a countermeasure should not be greater in cost than the risk it mitigates (ALE). For a quantitative risk assessment, the equation is ALE = ARO x SLE where the SLE is calculated as the product of asset value x exposure factor. An event that happen once every five years would have an ARO of .2 (1 divided by 5).
SLE = Asset Value (AV) x Exposure Fact (EF)
SLE = 1,000,000 x .30 = 300,000
ALE = SLE x Annualized Rate of Occurance (ARO)
ALE = 300,000 x .2 = 60,000
Know your acronyms:
ALE -- Annual loss expectancy
ARO -- Annual rate of occurrence
SLE -- Single loss expectancy
The following are incorrect answers:
$300,000 is incorrect. See the explanation of the correct answer for the correct calculation. $150,000 is incorrect. See the explanation of the correct answer for the correct calculation. $1,500 is incorrect. See the explanation of the correct answer for the correct calculation.
Reference(s) used for this question:
Mc Graw Hill, Shon Harris, CISSP All In One (AIO) book, Sixth Edition , Pages 87-88 and
Official ISC2 Guide to the CISSP Exam, (OIG), Pages 60-61

QUESTION 569
Which of the following statements pertaining to quantitative risk analysis is false?

A. Portion of it can be automated
B. It involves complex calculations
C. It requires a high volume of information
D. It requires little experience to apply

Correct Answer: D
Explanation

Explanation/Reference:

Explanation: Assigning the values for the inputs to a purely quantitative risk assessment requires both a lot of time and significant experience on the part of the assessors. The most experienced employees or representatives from each of the departments would be involved in the process. It is NOT an easy task if you wish to come up with accurate values. "It can be automated" is incorrect. There are a number of tools on the market that automate the process of conducting a quantitative risk assessment.
"It involves complex calculations" is incorrect. The calculations are simple for basic scenarios but could become fairly complex for large cases. The formulas have to be applied correctly. "It requires a high volume of information" is incorrect. Large amounts of information are required in order to develop reasonable and defensible values for the inputs to the quantitative risk assessment.
CBK, pp. 60-61
AIO3, p. 73, 78
The Cissp Prep Guide - Mastering The Ten Domains Of Computer Security - 2001, page 24

QUESTION 570

Notifying the appropriate parties to take action in order to determine the extent of the severity of an incident and to remediate the incident's effects is part of:

A. Incident Evaluation
B. Incident Recognition
C. Incident Protection
D. Incident Response

Correct Answer: D
Explanation

Explanation/Reference:

Explanation: These are core functions of the incident response process. "Incident Evaluation" is incorrect. Evaluation of the extent and cause of the incident is a component of the incident response process.
"Incident Recognition" is incorrect. Recognition that an incident has occurred is the precursor to the initiation of the incident response process.
"Incident Protection" is incorrect. This is an almost-right-sounding nonsense answer to distract the unwary.
References
CBK, pp. 698 - 703

QUESTION 571

An Intrusion Detection System (IDS) is what type of control?

A. A preventive control.
B. A detective control.
C. A recovery control.
D. A directive control.

Correct Answer: D
Explanation

Explanation/Reference:

Explanation: These controls can be used to investigate what happen after the fact. Your IDS may collect information on where the attack came from, what port was use, and other details that could be used in the investigation steps.
"Preventative control" is incorrect. Preventative controls preclude events or actions that might compromise a system or cause a policy violation. An intrusion prevention system would be an example of a preventative control.
"Recovery control" is incorrect. Recover controls include processes used to return the system to a secure state after the occurrence of a security incident. Backups and redundant components are examples of recovery controls.
"Directive controls" is incorrect. Directive controls are administrative instruments such as policies, procedures,

guidelines, and aggreements. An acceptable use policy is an example of a directive control.

CBK, pp. 646 - 647

QUESTION 572
To protect and/or restore lost, corrupted, or deleted information, thereby preserving the data integrity and availability is the purpose of:

A. Remote journaling.
B. Database shadowing.
C. A tape backup method.
D. Mirroring.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The purpose of a tape backup method is to protect and/or restore lost, corrupted, or deleted information, thereby preserving the data integrity and ensuring availability. All other choices could suffer from corruption and it might not be possible to restore the data without proper backups being done.
This is a tricky question, if the information is lost, corrupted, or deleted only a good backup could be use to restore the information. Any synchronization mechanism would update the mirror copy and the data could not be recovered.
With backups there could be a large gap where your latest data may not be available. You would have to look at your Recovery Point Objective and see if this is acceptable for your company recovery objectives.
The following are incorrect answers:
Mirroring will preserve integrity and restore points in all cases of drive failure. However, if you have corrupted data on the primary set of drives you may get corrupted data on the secondary set as well.
Remote Journaling provides Continuous or periodic synchronized recording of transaction data at a remote location as a backup strategy. (http://www.businessdictionary.com/definition/remotejournaling. html) With journaling there might be a gap of time between the data updates being send in batch at regular interval. So some of the data could be lost. Database shadowing is synonymous with Mirroring but it only applies to databases, but not to information and data as a whole.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 68.

QUESTION 573
Which of the following is NOT a task normally performed by a Computer Incident Response Team (CIRT)?

A. Develop an information security policy.
B. Coordinate the distribution of information pertaining to the incident to the appropriate parties.
C. Mitigate risk to the enterprise.
D. Assemble teams to investigate the potential vulnerabilities.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Writing a corporate security policy is normally a task of upper management in an organization. Other tasks would usually be performed by a Computer Incident Response Team. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 64).

QUESTION 574
Which of the following is NOT a common backup method?

A. Full backup method
B. Daily backup method
C. Incremental backup method
D. Differential backup method

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: A daily backup is not a backup method, but defines periodicity at which backups are made. There can be daily full, incremental or differential backups. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 69).

QUESTION 575
Which backup method only copies files that have been recently added or changed and also leaves the archive bit unchanged?

A. Full backup method
B. Incremental backup method
C. Fast backup method
D. Differential backup method

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: A differential backup is a partial backup that copies a selected file to tape only if the archive bit for that file is turned on, indicating that it has changed since the last full backup. A differential backup leaves the archive bits unchanged on the files it copies. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 69).
Also see: http://e-articles.info/e/a/title/Backup-Types/ Backup software can use or ignore the archive bit in determining which files to back up, and can either turn the archive bit off or leave it unchanged when the backup is complete. How the archive bit is used and manipulated determines what type of backup is done, as follows Full backup
A full backup, which Microsoft calls a normal backup, backs up every selected file, regardless of the status of the archive bit. When the backup completes, the backup software turns off the archive bit for every file that was backed up. Note that "full" is a misnomer because a full backup backs up only the files you have selected, which may be as little as one directory or even a single file, so in that sense Microsoft's terminology is actually more accurate. Given the choice, full backup is the method to use because all files are on one tape, which makes it much easier to retrieve files from tape when necessary. Relative to partial backups, full backups also increase redundancy because all files are on all tapes. That means that if one tape fails, you may still be able to retrieve a given file from another tape.
Differential backup
A differential backup is a partial backup that copies a selected file to tape only if the archive bit for that file is turned on, indicating that it has changed since the last full backup. A differential backup leaves the archive bits unchanged on the files it copies. Accordingly, any differential backup set contains all files that have changed since the last full backup. A differential backup set run soon after a full backup will contain relatively few files. One run soon before the next full backup is due will contain many files, including those contained on all previous differential backup sets since the last full backup. When you use differential backup, a complete backup set comprises only two tapes or tape sets: the tape that contains the last full backup and the tape that contains the most recent differential backup.
Incremental backup
An incremental backup is another form of partial backup. Like differential backups, Incremental Backups copy a selected file to tape only if the archive bit for that file is turned on. Unlike the differential backup, however, the incremental backup clears the archive bits for the files it backs up. An incremental backup set therefore

contains only files that have changed since the last full backup or the last incremental backup. If you run an incremental backup daily, files changed on Monday are on the Monday tape, files changed on Tuesday are on the Tuesday tape, and so forth. When you use an incremental backup scheme, a complete backup set comprises the tape that contains the last full backup and all of the tapes that contain every incremental backup done since the last normal backup. The only advantages of incremental backups are that they minimize backup time and keep multiple versions of files that change frequently. The disadvantages are that backed-up files are scattered across multiple tapes, making it difficult to locate any particular file you need to restore, and that there is no redundancy. That is, each file is stored only on one tape.
Full copy backup
A full copy backup (which Microsoft calls a copy backup) is identical to a full backup except for the last step. The full backup finishes by turning off the archive bit on all files that have been backed up. The full copy backup instead leaves the archive bits unchanged. The full copy backup is useful only if you are using a combination of full backups and incremental or differential partial backups. The full copy backup allows you to make a duplicate "full" backup--e.g., for storage offsite, without altering the state of the hard drive you are backing up, which would destroy the integrity of the partial backup rotation.
Some Microsoft backup software provides a bizarre backup method Microsoft calls a daily copy backup. This method ignores the archive bit entirely and instead depends on the date- and timestamp of files to determine which files should be backed up. The problem is, it's quite possible for software to change a file without changing the date- and timestamp, or to change the date- and timestamp without changing the contents of the file. For this reason, we regard the daily copy backup as entirely unreliable and recommend you avoid using it.

QUESTION 576
Which backup method does not reset the archive bit on files that are backed up?

A. Full backup method
B. Incremental backup method
C. Differential backup method
D. Additive backup method

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The differential backup method only copies files that have changed since the last full backup was performed. It is additive in the fact that it does not reset the archive bit so all changed or added files are backed up in every differential backup until the next full backup. The "additive backup method" is not a common backup method.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 69).

QUESTION 577
Which common backup method is the fastest on a daily basis?

A. Full backup method
B. Incremental backup method
C. Fast backup method
D. Differential backup method

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The incremental backup method only copies files that have been recently changed or added. Only files with their archive bit set are backed up. This method is fast and uses less tape space but has some inherent vulnerabilities, one being that all incremental backups need to be available and restored from the date of the last full backup to the desired date should a restore be needed.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 69).

QUESTION 578
Which of the following backup methods is most appropriate for off-site archiving?

A. Incremental backup method
B. Off-site backup method
C. Full backup method
D. Differential backup method

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The full backup makes a complete backup of every file on the system every time it is run. Since a single backup set is needed to perform a full restore, it is appropriate for off-site archiving.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 69).

QUESTION 579
Which of the following tasks is NOT usually part of a Business Impact Analysis (BIA)?

A. Calculate the risk for each different business function.
B. Identify the company's critical business functions.
C. Calculate how long these functions can survive without these resources.
D. Develop a mission statement.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The Business Impact Analysis is critical for the development of a business continuity plan (BCP). It identifies risks, critical processes and resources needed in case of recovery and quantifies the impact a disaster will have upon the organization. The development of a mission statement is normally performed before the BIA.
A BIA (business impact analysis) is considered a functional analysis, in which a team collects data through interviews and documentary sources; documents business functions, activities, and transactions ; develops a hierarchy of business functions; and finally applies a classification scheme to indicate each individual function's criticality level.
BIA Steps
The more detailed and granular steps of a BIA are outlined here:
1. Select individuals to interview for data gathering.
2. Create data-gathering techniques (surveys, questionnaires, qualitative and quantitative approaches).
3. Identify the company's critical business functions.
4. Identify the resources these functions depend upon.
5. Calculate how long these functions can survive without these resources.
6. Identify vulnerabilities and threats to these functions.
7. Calculate the risk for each different business function.
8. Document findings and report them to management.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Location 21076). Auerbach Publications. Kindle Edition.
and
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 905-910). McGraw-Hill.

Kindle Edition.

QUESTION 580
Which of the following is an example of an active attack?

A. Traffic analysis
B. Scanning
C. Eavesdropping
D. Wiretapping

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Scanning is definitively a very active attack. The attacker will make use of a scanner to perform the attack, the scanner will send a very large quantity of packets to the target in order to illicit responses that allows the attacker to find information about the operating system, vulnerabilities, misconfiguration and more. The packets being sent are sometimes attempting to identify if a known vulnerability exist on the remote hosts.
A passive attack is usually done in the footprinting phase of an attack. While doing your passive reconnaissance you never send a single packet to the destination target. You gather information from public databases such as the DNS servers, public information through search engines, financial information from finance web sites, and technical infomation from mailing list archive or job posting for example.
An attack can be active or passive.
An "active attack" attempts to alter system resources or affect their operation. A "passive attack" attempts to learn or make use of information from the system but does not affect system resources. (E.g., see: wiretapping.)
The following are all incorrect answers because they are all passive attacks:
Traffic Analysis - Is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed in the context of military intelligence or counter-intelligence, and is a concern in computer security.
Eavesdropping - Eavesdropping is another security risk posed to networks. Because of the way some networks are built, anything that gets sent out is broadcast to everyone. Under normal circumstances, only the computer that the data was meant for will process that information. However, hackers can set up programs on their computers called "sniffers" that capture all data being broadcast over the network. By carefully examining the data, hackers can often reconstruct real data that was never meant for them. Some of the most damaging things that get sniffed include passwords and credit card information.
In the cryptographic context, Eavesdropping and sniffing data as it passes over a network are considered passive attacks because the attacker is not affecting the protocol, algorithm, key, message, or any parts of the encryption system. Passive attacks are hard to detect, so in most cases methods are put in place to try to prevent them rather than to detect and stop them. Altering messages, modifying system files, and masquerading as another individual are acts that are considered active attacks because the attacker is actually doing something instead of sitting back and gathering data. Passive attacks are usually used to gain information prior to carrying out an active attack."
Wiretapping - Wiretapping refers to listening in on electronic communications on telephones, computers, and other devices. Many governments use it as a law enforcement tool, and it is also used in fields like corporate espionage to gain access to privileged information. Depending on where in the world one is, wiretapping may be tightly controlled with laws that are designed to protect privacy rights, or it may be a widely accepted practice with little or no protections for citizens. Several advocacy organizations have been established to help civilians understand these laws in their areas, and to fight illegal wiretapping.
Reference(s) used for this question:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 6th Edition, Cryptography, Page 865 and
http://en.wikipedia.org/wiki/Attack_%28computing%29
and
http://www.wisegeek.com/what-is-wiretapping.htm
and
https://pangea.stanford.edu/computing/resources/network/security/risks.php and

http://en.wikipedia.org/wiki/Traffic_analysis

QUESTION 581
What can be defined as a momentary low voltage?

A. Spike
B. Sag
C. Fault
D. Brownout

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: A sag is a momentary low voltage. A spike is a momentary high voltage. A fault is a momentary power out and a brownout is a prolonged power supply that is below normal voltage. Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 6: Physical security (page 299)

QUESTION 582
The absence of a safeguard, or a weakness in a system that may possibly be exploited is called a(n)?

A. Threat
B. Exposure
C. Vulnerability
D. Risk

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: A vulnerability is a weakness in a system that can be exploited by a threat. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 237.

QUESTION 583
Which of the following statements pertaining to disk mirroring is incorrect?

A. Mirroring offers better performance in read operations but writing hinders system performance.
B. Mirroring is a hardware-based solution only.
C. Mirroring offers a higher fault tolerance than parity.
D. Mirroring is usually the less cost-effective solution.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: With mirroring, the system writes the data simultaneously to separate drives or arrays.
The advantage of mirroring are minimal downtime, simple data recovery, and increased performance in reading from the disk.
The disadvantage of mirroring is that both drives or disk arrays are processing in the writing to disks function, which can hinder system performance.
Mirroring has a high fault tolerance and can be implemented either through a hardware RAID controller or through the operating system. Since it requires twice the disk space than actual data, mirroring is the less cost-efficient data redundancy strategy. Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology

Systems, December 2001 (page 45).

QUESTION 584
Which of the following is NOT a common category/classification of threat to an IT system?

A. Human
B. Natural
C. Technological
D. Hackers

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Hackers are classified as a human threat and not a classification by itself. All the other answers are incorrect. Threats result from a variety of factors, although they are classified in three types: Natural (e.g., hurricane, tornado, flood and fire), human (e.g. operator error, sabotage, malicious code) or technological (e.g. equipment failure, software error, telecommunications network outage, electric power failure). SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf, June 2002 (page 6).

QUESTION 585
Which of the following enables the person responsible for contingency planning to focus risk management efforts and resources in a prioritized manner only on the identified risks?

A. Risk assessment
B. Residual risks
C. Security controls
D. Business units

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The risk assessment is critical because it enables the person responsible for contingency planning to focus risk management efforts and resources in a prioritized manner only on the identified risks. The risk management process includes the risk assessment and determination of suitable technical, management, and operational security controls based on the level of threat the risk imposes. Business units should be included in this process. Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 7).

QUESTION 586
A contingency plan should address:

A. Potential risks.
B. Residual risks.
C. Identified risks.
D. All answers are correct.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Because it is rarely possible or cost effective to eliminate all risks, an attempt is made to reduce risks to an acceptable level through the risk assessment process. This process allows, from a set of potential

risks (whether likely or not), to come up with a set of identified, possible risks.
The implementation of security controls allows reducing the identified risks to a smaller set of residual risks. Because these residual risks represent the complete set of situations that could affect system performance, the scope of the contingency plan may be reduced to address only this decreased risk set.
As a result, the contingency plan can be narrowly focused, conserving resources while ensuring an effective system recovery capability.
Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 7).

QUESTION 587
Which of the following focuses on sustaining an organization's business functions during and after a disruption?

A. Business continuity plan
B. Business recovery plan
C. Continuity of operations plan
D. Disaster recovery plan

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: A business continuity plan (BCP) focuses on sustaining an organization's business functions during and after a disruption. Information systems are considered in the BCP only in terms of their support to the larger business processes. The business recovery plan (BRP) addresses the restoration of business processes after an emergency. The BRP is similar to the BCP, but it typically lacks procedures to ensure continuity of critical processes throughout an emergency or disruption. The continuity of operations plan (COOP) focuses on restoring an organization's essential functions at an alternate site and performing those functions for up to 30 days before returning to normal operations. The disaster recovery plan (DRP) applies to major, usually catastrophic events that deny access to the normal facility for an extended period. A DRP is narrower in scope than an IT contingency plan in that it does not address minor disruptions that do not require relocation.
Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 8).

QUESTION 588
Which of the following specifically addresses cyber attacks against an organization's IT systems?

A. Continuity of support plan
B. Business continuity plan
C. Incident response plan
D. Continuity of operations plan

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The incident response plan focuses on information security responses to incidents affecting systems and/or networks. It establishes procedures to address cyber attacks against an organization's IT systems. These procedures are designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized access to a system or data, denial of service, or unauthorized changes to system hardware or software. The continuity of support plan is the same as an IT contingency plan. It addresses IT system disruptions and establishes procedures for recovering a major application or general support system. It is not business process focused. The business continuity plan addresses business processes and provides procedures for sustaining essential business operations while

recovering from a significant disruption. The continuity of operations plan addresses the subset of an organization's missions that are deemed most critical and procedures to sustain these functions at an alternate site for up to 30 days.
Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 8).

QUESTION 589
In which of the following phases of system development life cycle (SDLC) is contingency planning most important?

A. Initiation
B. Development/acquisition
C. Implementation
D. Operation/maintenance

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Contingency planning requirements should be considered at every phase of SDLC, but most importantly when a new IT system is being conceived. In the initiation phase, system requirements are identified and matched to their related operational processes, allowing determination of the system's appropriate recovery priority. Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 12).
and
The Official ISC2 Guide to the CBK, Second Edition, Application Security, page 180-185

QUESTION 590
Which of the following teams should NOT be included in an organization's contingency plan?

A. Damage assessment team
B. Hardware salvage team
C. Tiger team
D. Legal affairs team

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: According to NIST's Special publication 800-34, a capable recovery strategy will require some or all of the following functional groups: Senior management official, management team, damage assessment team, operating system administration team, systems software team, server recovery team, LAN/WAN recovery team, database recovery team, network operations recovery team, telecommunications team, hardware salvage team, alternate site recovery coordination team, original site restoration/salvage coordination team, test team, administrative support team, transportation and relocation team, media relations team, legal affairs team, physical/personal security team, procurements team. Ideally, these teams would be staffed with the personnel responsible for the same or similar operation under normal conditions. A tiger team, originally a U.S. military jargon term, defines a team (of sneakers) whose purpose is to penetrate security, and thus test security measures. Used today for teams performing ethical hacking. Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 23).

QUESTION 591
Which of the following statements pertaining to the maintenance of an IT contingency plan is incorrect?

A. The plan should be reviewed at least once a year for accuracy and completeness.
B. The Contingency Planning Coordinator should make sure that every employee gets an up-todate copy of the plan.
C. Strict version control should be maintained.
D. Copies of the plan should be provided to recovery personnel for storage offline at home and office.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Because the contingency plan contains potentially sensitive operational and personnel information, its distribution should be marked accordingly and controlled. Not all employees would obtain a copy, but only those involved in the execution of the plan.
All other statements are correct.
NOTE FROM CLEMENT:
I have received multiple emails stating the explanations contradict the correct answer. It seems many people have a hard time with negative question. In this case the Incorrect choice (the one that is not true) is the correct choice. Be very carefull of such questions, you will get some on the real exam as well.
Reference(s) used for this question:
SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems

QUESTION 592
Which of the following is less likely to accompany a contingency plan, either within the plan itself or in the form of an appendix?

A. Contact information for all personnel.
B. Vendor contact information, including offsite storage and alternate site.
C. Equipment and system requirements lists of the hardware, software, firmware and other resources required to support system operations.
D. The Business Impact Analysis.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Why is this the correct answer? Simply because it is WRONG, you would have contact information for your emergency personnel within the plan but NOT for ALL of your personnel. Be careful of words such as ALL.
According to NIST's Special publication 800-34, contingency plan appendices provide key details not contained in the main body of the plan. The appendices should reflect the specific technical, operational, and management contingency requirements of the given system. Contact information for recovery team personnel (not all personnel) and for vendor should be included, as well as detailed system requirements to allow for supporting of system operations. The Business Impact Analysis (BIA) should also be included as an appendix for reference should the plan be activated.
Reference(s) used for this question:
SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems

QUESTION 593
Which of the following server contingency solutions offers the highest availability?

A. System backups
B. Electronic vaulting/remote journaling
C. Redundant arrays of independent disks (RAID)
D. Load balancing/disk replication

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Of the offered technologies, load balancing/disk replication offers the highest availability, measured in terms of minutes of lost data or server downtime. A Network-Attached Storage (NAS) or a Storage Area Network (SAN) solution combined with virtualization would offer an even higher availability.
Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 49).

QUESTION 594
What assesses potential loss that could be caused by a disaster?

A. The Business Assessment (BA)
B. The Business Impact Analysis (BIA)
C. The Risk Assessment (RA)
D. The Business Continuity Plan (BCP)

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The Business Assessment is divided into two components. Risk Assessment (RA) and Business Impact Analysis (BIA). Risk Assessment is designed to evaluate existing exposures from the organization's environment, whereas the BIA assesses potential loss that could be caused by a disaster. The Business Continuity Plan's goal is to reduce the risk of financial loss by improving the ability to recover and restore operations efficiently and effectively. Source: BARNES, James C. & ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 57).
And: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 276).

QUESTION 595
Which of the following item would best help an organization to gain a common understanding of functions that are critical to its survival?

A. A risk assessment
B. A business assessment
C. A disaster recovery plan
D. A business impact analysis

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: A Business Impact Analysis (BIA) is an assessment of an organization's business functions to develop an understanding of their criticality, recovery time objectives, and resources needed.
By going through a Business Impact Analysis, the organization will gain a common understanding of functions that are critical to its survival.
A risk assessment is an evaluation of the exposures present in an organization's external and internal environments.
A Business Assessment generally include Business Analysis as a discipline and it has heavy overlap with requirements analysis sometimes also called requirements engineering, but focuses on identifying the changes to an organization that are required for it to achieve strategic goals. These changes include changes to strategies, structures, policies, processes, and information systems.

A disaster recovery plan is the comprehensive statement of consistent actions to be taken before, during and after a disruptive event that causes a significant loss of information systems resources. Source: BARNES, James C. & ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 57).

QUESTION 596
What can be defined as the maximum acceptable length of time that elapses before the unavailability of the system severely affects the organization?

A. Recovery Point Objectives (RPO)
B. Recovery Time Objectives (RTO)
C. Recovery Time Period (RTP)
D. Critical Recovery Time (CRT)

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: One of the results of a Business Impact Analysis is a determination of each business function's Recovery Time Objectives (RTO). The RTO is the amount of time allowed for the recovery of a business function. If the RTO is exceeded, then severe damage to the organization would result.
The Recovery Point Objectives (RPO) is the point in time in which data must be restored in order to resume processing.
Reference(s) used for this question:
BARNES, James C. & ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 68).
and
And: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 47).

QUESTION 597
Which of the following steps should be one of the first step performed in a Business Impact Analysis (BIA)?

A. Identify all CRITICAL business units within the organization.
B. Evaluate the impact of disruptive events.
C. Estimate the Recovery Time Objectives (RTO).
D. Identify and Prioritize Critical Organization Functions

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Project Initiation and Management
This is the first step in building the Business Continuity program is project initiation and management. During this phase, the following activities will occur:
Obtain senior management support to go forward with the project Define a project scope, the objectives to be achieved, and the planning assumptions Estimate the project resources needed to be successful, both human resources and financial resources
Define a timeline and major deliverables of the project In this phase, the program will be managed like a project, and a project manager should be assigned to the BC and DR domain. The next step in the planning process is to have the planning team perform a BI A. The BIA will
help the company decide what needs to be recovered, and how quickly. Mission functions are typically designated with terms such as critical, essential, supporting and nonessential to help determine the appropriate prioritization.
One of the first steps of a BIA is to Identify and Prioritize Critical Organization Functions. All organizational functions and the technology that supports them need to be classified based on their recovery priority.

Recovery time frames for organization operations are driven by the consequences of not performing the function. The consequences may be the result of organization lost during the down period; contractual commitments not met resulting in fines or lawsuits, lost goodwill with customers.
All other answers are incorrect.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 21073-21075). Auerbach Publications. Kindle Edition. Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 20697-20710). Auerbach Publications. Kindle Edition.

QUESTION 598
A business continuity plan should list and prioritize the services that need to be brought back after a disaster strikes. Which of the following services is more likely to be of primary concern in the context of what your Disaster Recovery Plan would include?

A. Marketing/Public relations
B. Data/Telecomm/IS facilities
C. IS Operations
D. Facilities security

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The main concern when recovering after a disaster is data, telecomm and IS facilities. Other services, in descending priority order are: IS operations, IS support services, market structure, marketing/ public relations, customer service & systems support, market regulation/surveillance, listing, application development, accounting services, facilities, human resources, facilities security, legal and Office of the Secretary, national sales. Source: BARNES, James C. & ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 129).

QUESTION 599
During the salvage of the Local Area Network and Servers, which of the following steps would normally be performed first?

A. Damage mitigation
B. Install LAN communications network and servers
C. Assess damage to LAN and servers
D. Recover equipment

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The first activity in every recovery plan is damage assessment, immediately followed by damage mitigation.
This first activity would typically include assessing the damage to all network and server components (including cables, boards, file servers, workstations, printers, network equipment), making a list of all items to be repaired or replaced, selecting appropriate vendors and relaying findings to Emergency Management Team.
Following damage mitigation, equipment can be recovered and LAN communications network and servers can be reinstalled.
Source: BARNES, James C. & ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 135).

QUESTION 600
Which of the following rules pertaining to a Business Continuity Plan/Disaster Recovery Plan is incorrect?

A. In order to facilitate recovery, a single plan should cover all locations.

B. There should be requirements to form a committee to decide a course of action. These decisions should be made ahead of time and incorporated into the plan.

C. In its procedures and tasks, the plan should refer to functions, not specific individuals.

D. Critical vendors should be contacted ahead of time to validate equipment can be obtained in a timely manner.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The first documentation rule when it comes to a BCP/DRP is "one plan, one building". Much of the plan revolves around reconstructing a facility and replenishing it with production contents. If more than one facility is involved, then the reader of the plan will find it difficult to identify quantities and specifications of replacement resource items. It is possible to have multiple plans for a single building, but those plans must be linked so that the identification and ordering of resource items is centralized. All other statements are correct.
Source: BARNES, James C. & ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 162).

Exam B

QUESTION 1
A Business Continuity Plan should be tested:

A. Once a month.
B. At least twice a year.
C. At least once a year.
D. At least once every two years.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: It is recommended that testing does not exceed established frequency limits. For a plan to be effective, all components of the BCP should be tested at least once a year. Also, if there is a major change in the operations of the organization, the plan should be revised and tested not more than three months after the change becomes operational. Source: BARNES, James C. & ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 165).

QUESTION 2
Which of the following statements pertaining to a Criticality Survey is incorrect?

A. It is implemented to gather input from all personnel that is going to be part of the recovery teams.
B. The purpose of the survey must be clearly stated.
C. Management's approval should be obtained before distributing the survey.
D. Its intent is to find out what services and systems are critical to keeping the organization in business.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The Criticality Survey is implemented through a standard questionnaire to gather input from the most knowledgeable people. Not all personnel that is going to be part of recovery teams is necessarily able to help in identifying critical functions of the organization. The intent of such a survey is to identify the services and systems that are critical to the organization.
Having a clearly stated purpose for the survey helps in avoiding misinterpretations. Management's approval of the survey should be obtained before distributing it. Source: HARE, Chris, CISSP Study Guide: Business Continuity Planning Domain,

QUESTION 3
Which disaster recovery plan test involves functional representatives meeting to review the plan in detail?

A. Simulation test
B. Checklist test
C. Parallel test
D. Structured walk-through test

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The structured walk-through test occurs when the functional representatives meet to review the plan in detail. This involves a thorough look at each of the plan steps, and the procedures that are invoked at that point in the plan. This ensures that the actual planned activities are accurately described in the plan. The checklist test is a method of testing the plan by distributing copies to each of the functional areas. The

simulation test plays out different scenarios. The parallel test is essentially an operational test that is performed without interrupting current processing.
Source: HARE, Chris, CISSP Study Guide: Business Continuity Planning Domain,

QUESTION 4
The criteria for evaluating the legal requirements for implementing safeguards is to evaluate the cost (C) of instituting the protection versus the estimated loss (L) resulting from the exploitation of the corresponding vulnerability. Therefore, a legal liability may exists when:

A. (C < L) or C is less than L
B. (C < L - (residual risk)) or C is less than L minus residual risk
C. (C > L) or C is greather than L
D. (C > L - (residual risk)) or C is greather than L minus residual risk

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: If the cost is lower than the estimated loss (C < L), then legal liability may exists if you fail to implement the proper safeguards.
Government laws and regulations require companies to employ reasonable security measures to reduce private harms such as identity theft due to unauthorized access. The U.S. Gramm-Leach- Bliley Act (GLBA) Safeguards Rule and the broader European Directive 95/46/EC, Article 17, both require that companies employ reasonable or
appropriate administrative and technical security measures to protect consumer information. The GLBA is a U.S. Federal law enacted by U.S. Congress in 1998 to allow consolidation among commercial banks. The GLBA Safeguards Rule is U.S. Federal regulation created in reaction to the GLBA and enforced by the U.S. Federal Trade Commission (FTC). The Safeguards Rule requires companies to implement a security plan to protect the confidentiality and integrity of consumer personal information and requires the designation of an individual responsible for compliance. Because these laws and regulations govern consumer personal information, they can lead to new requirements for information systems for which companies are responsible to comply. The act of compliance includes demonstrating due diligence, which is defined as "reasonable efforts that persons make to satisfy legal requirements or discharge their legal obligations". Reasonableness in software systems includes industries standards and may allow for imperfection. Lawyers representing firms and other organizations, regulators, system administrators and engineers all face considerable challenge in determining what constitutes "reasonable" security measures for several reasons, including:
1. Compliance changes with the emergence of new security vulnerabilities due to innovations in information technology;
2. Compliance requires knowledge of specific security measures, however publicly available best practices typically include general goals and only address broad categories of vulnerability; and
3. Compliance is a best-effort practice, because improving security is costly and companies must prioritize security spending commensurate with risk of non-compliance. In general, the costs of improved security are certain, but the
improvement in security depends on unknown variables and probabilities outside the control of companies.
The following reference(s) were used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 315.
and
http://www.cs.cmu.edu/~breaux/publications/tdbreaux-cose10.pdf

QUESTION 5
What is called an exception to the search warrant requirement that allows an officer to conduct a search without having the warrant in-hand if probable cause is present and destruction of the evidence is deemed imminent?

A. Evidence Circumstance Doctrine
B. Exigent Circumstance Doctrine

C. Evidence of Admissibility Doctrine

D. Exigent Probable Doctrine

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: An Exigent Circumstance is an unusual and time-sensitive circumstance that justifies conduct that might not be permissible or lawful in other circumstances. For example, exigent circumstances may justify actions by law enforcement officers acting without a warrant such as a mortal danger to a young child.
Examples of other exigent circumstances include protecting evidence or property from imminent destruction. In US v Martinez, Justice Thomas of the United States Court of Appeal used these words:
"As a general rule, we define exigent circumstances as those circumstances that would cause a reasonable person to believe that entry was necessary to prevent physical harm to the officers or other persons, the destruction of relevant evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts." In Alvarado, Justice Blackburn of the Court of Appeals of Georgia referred to exigent circumstances in the context of a drug bust:
"The exigent circumstance doctrine provides that when probable cause has been established to believe that evidence will be removed or destroyed before a warrant can be obtained, a warrantless search and seizure can be justified. As many courts have noted, the need for the exigent circumstance doctrine is particularly compelling in narcotics cases, because contraband and records can be easily and quickly destroyed while a search is progressing. Police officers relying on this exception must demonstrate an objectively reasonable basis for deciding that immediate action is required."
All of the other answers were only detractors made up and not legal terms.
Reference(s) used for this question:
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 313.
and
http://www.duhaime.org/LegalDictionary/E/ExigentCircumstances.aspx

QUESTION 6
A copy of evidence or oral description of its contents; which is not as reliable as best evidence is what type of evidence?

A. Direct evidence

B. Circumstantial evidence

C. Hearsay evidence

D. Secondary evidence

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Secondary evidence is a copy of evidence or oral description of its contents; not as reliable as best evidence
Here are other types of evidence:
Best evidence -- original or primary evidence rather than a copy of duplicate of the evidence Direct evidence -- proves or disproves a specific act through oral testimony based on information gathered through the witness's five senses
Conclusive evidence -- incontrovertible; overrides all other evidence Opinions -- two types: Expert -- may offer an opinion based on personal expertise and facts, Non-expert -- may testify only as to facts
Circumstantial evidence -- inference of information from other, immediate, relevant facts Corroborative evidence -- supporting evidence used to help prove an idea or point; used as a supplementary tool to help prove a primary piece of evidence Hearsay evidence (3rdparty) -- oral or written evidence that is presented in court that is second hand and has no firsthand proof of accuracy or reliability (i) Usually not admissible in court (ii) Computer generated records and other business records are in hearsay category (iii) Certain exceptions to hearsay rule:
(1) Made during the regular conduct of business and authenticated by witnesses familiar with their use

(2) Relied upon in the regular course of business
(3) Made by a person with knowledge of records
(4) Made by a person with information transmitted by a person with knowledge (5) Made at or near the time of occurrence of the act being investigated (6) In the custody of the witness on a regular basis
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 310.
and
CISSP for Dummies, Peter Gregory, page 270-271

QUESTION 7
Which of the following proves or disproves a specific act through oral testimony based on information gathered through the witness's five senses?

A. Direct evidence.
B. Circumstantial evidence.
C. Conclusive evidence.
D. Corroborative evidence.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Direct evidence can prove a fact all by itself and does not need backup information to refer to. When using direct evidence, presumptions are not required. One example of direct evidence is the testimony of a witness who saw a crime take place. Although this oral evidence would be secondary in nature, meaning a case could not rest on just it alone, it is also direct evidence, meaning the lawyer does not necessarily need to provide other evidence to back it up. Direct evidence often is based on information gathered from a witness's five senses.
The following answers are incorrect:
Circumstantial evidence. Is incorrect because Circumstantial evidence can prove an intermediate fact that can then be used to deduce or assume the existence of another fact. Conclusive evidence. Is incorrect because Conclusive evidence is irrefutable and cannot be contradicted. Conclusive evidence is very strong all by itself and does not require corroboration. Corroborative evidence. Is incorrect because Corroborative evidence is supporting evidence used to help prove an idea or point. It cannot stand on its own, but is used as a supplementary tool to help prove a primary piece of evidence.

QUESTION 8
This type of supporting evidence is used to help prove an idea or a point, however It cannot stand on its own, it is used as a supplementary tool to help prove a primary piece of evidence. What is the name of this type of evidence?

A. Circumstantial evidence
B. Corroborative evidence
C. Opinion evidence
D. Secondary evidence

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: This type of supporting evidence is used to help prove an idea or a point, however It cannot stand on its own, it is used as a supplementary tool to help prove a primary piece of evidence. Corrobative evidence takes many forms.
In a rape case for example, this could consist of torn clothing, soiled bed sheets, 911 emergency calls tapes, and
prompt complaint witnesses.
There are many types of evidence that exist. Below you have explanations of some of the most common types:

Physical Evidence

Physical evidence is any evidence introduced in a trial in the form of a physical object, intended to prove a fact in issue based on its demonstrable physical characteristics. Physical evidence can conceivably include all or part of any object.

In a murder trial for example (or a civil trial for assault), the physical evidence might include DNA left by the attacker on the victim's body, the body itself, the weapon used, pieces of carpet spattered with blood, or casts of footprints or tire prints found at the scene of the crime.

Real Evidence

Real evidence is a type of physical evidence and consists of objects that were involved in a case or actually played a part in the incident or transaction in question. Examples include the written contract, the defective part or defective product, the murder weapon, the gloves used by an alleged murderer. Trace evidence, such as fingerprints and firearm residue, is a species of real evidence. Real evidence is usually reported upon by an expert witness with appropriate qualifications to give an opinion. This normally means a forensic scientist or one qualified in forensic engineering.

Admission of real evidence requires authentication, a showing of relevance, and a showing that the object is in "the same or substantially the same condition" now as it was on the relevant date. An object of real evidence is authenticated through the senses of witnesses or by circumstantial evidence called chain of custody.

Documentary

Documentary evidence is any evidence introduced at a trial in the form of documents. Although this term is most widely understood to mean writings on paper (such as an invoice, a contract or a will), the term actually include any media by which information can be preserved. Photographs, tape recordings, films, and printed emails are all forms of documentary evidence.

Documentary versus physical evidence

A piece of evidence is not documentary evidence if it is presented for some purpose other than the examination of the contents of the document. For example, if a blood-spattered letter is introduced solely to show that the defendant stabbed the author of the letter from behind as it was being written, then the evidence is physical evidence, not documentary evidence. However, a film of the murder taking place would be documentary evidence (just as a written description of the event from an eyewitness). If the content of that same letter is then introduced to show the motive for the murder, then the evidence would be both physical and documentary.

Documentary Evidence Authentication

Documentary evidence is subject to specific forms of authentication, usually through the testimony of an eyewitness to the execution of the document, or to the testimony of a witness able to identify the handwriting of the purported author. Documentary evidence is also subject to the best evidence rule, which requires that the original document be produced unless there is a good reason not to do so.

The role of the expert witness

Where physical evidence is of a complexity that makes it difficult for the average person to understand its significance, an expert witness may be called to explain to the jury the proper interpretation of the evidence at hand.

Digital Evidence or Electronic Evidence

Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial.

The use of digital evidence has increased in the past few decades as courts have allowed the use of e-mails, digital photographs, ATM transaction logs, word processing documents, instant message histories, files saved from accounting programs, spreadsheets, internet browser histories, databases, the contents of computer memory, computer backups, computer printouts, Global Positioning System tracks, logs from a hotel's electronic door locks, and digital video or audio files.

While many courts in the United States have applied the Federal Rules of Evidence to digital evidence in the same way as more traditional documents, courts have noted very important differences. As compared to the more traditional evidence, courts have noted that digital evidence tends to be more voluminous, more difficult to destroy, easily modified, easily duplicated, potentially more expressive, and more readily available. As such, some courts have sometimes treated digital evidence differently for purposes of authentication, hearsay, the best evidence rule, and privilege. In December 2006, strict new rules were enacted within the Federal Rules of Civil Procedure requiring the preservation and disclosure of electronically stored evidence.

Demonstrative Evidence

Demonstrative evidence is evidence in the form of a representation of an object. This is, as opposed to, real evidence, testimony, or other forms of evidence used at trial. Examples of demonstrative evidence include photos, x-rays, videotapes, movies, sound recordings, diagrams, forensic animation, maps, drawings, graphs, animation, simulations, and models. It is useful for assisting a finder of fact (fact-finder) in establishing context among the facts presented in a case. To be admissible, a demonstrative exhibit must "fairly and accurately" represent the real object at the relevant time.

Chain of custody

Chain of custody refers to the chronological documentation, and/or paper trail, showing the seizure, custody, control, transfer, analysis, and disposition of evidence, physical or electronic. Because evidence can be used in court to convict persons of crimes, it must be handled in a scrupulously careful manner to avoid later allegations of tampering or misconduct which can compromise the case of the prosecution toward acquittal or to overturning a guilty verdict upon appeal.

The idea behind recoding the chain of custody is to establish that the alleged evidence is fact related to the alleged crime - rather than, for example, having been planted fraudulently to make someone appear guilty.

Establishing the chain of custody is especially important when the evidence consists of fungible goods. In practice, this most often applies to illegal drugs which have been seized by law enforcement personnel. In such cases, the defendant at times disclaims any knowledge of possession of the controlled substance in question.

Accordingly, the chain of custody documentation and testimony is presented by the prosecution to establish that the substance in evidence was in fact in the possession of the defendant. An identifiable person must always have the physical custody of a piece of evidence. In practice, this means that a police officer or detective will take charge of a piece of evidence, document its collection, and hand it over to an evidence clerk for storage in a secure place. These transactions, and every succeeding transaction between the collection of the evidence and its appearance in court, should be completely documented chronologically in order to withstand legal challenges to the authenticity of the evidence. Documentation should include the conditions under which the evidence is gathered, the identity of all evidence handlers, duration of evidence custody, security conditions while handling or storing the evidence, and the manner in which evidence is transferred to subsequent custodians each time such a transfer occurs (along with the signatures of persons involved at each step).

Example

An example of "Chain of Custody" would be the recovery of a bloody knife at a murder scene:

Officer Andrew collects the knife and places it into a container, then gives it to forensics technician Bill.

Forensics technician Bill takes the knife to the lab and collects fingerprints and other evidence from the knife.

Bill then gives the knife and all evidence gathered from the knife to evidence clerk Charlene. Charlene then stores the evidence until it is needed, documenting everyone who has accessed the original evidence (the knife, and original copies of the lifted fingerprints). The Chain of Custody requires that from the moment the evidence is collected, every transfer of evidence from person to person be documented and that it be provable that nobody else could have accessed that evidence. It is best to keep the number of transfers as low as possible. In the courtroom, if the defendant questions the Chain of Custody of the evidence it can be proven that the knife in the evidence room is the same knife found at the crime scene. However, if there are discrepancies and it cannot be proven who had the knife at a particular point in time, then the Chain of Custody is broken and the defendant can ask to have the resulting evidence declared inadmissible.

"Chain of custody" is also used in most chemical sampling situations to maintain the integrity of the sample by providing documentation of the control, transfer, and analysis of samples. Chain of custody is especially important in environmental work where sampling can identify the existence of contamination and can be used to identify the responsible party.

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 23173-23185). Auerbach Publications. Kindle Edition.
http://en.wikipedia.org/wiki/Documentary_evidence
http://en.wikipedia.org/wiki/Physical_evidence
http://en.wikipedia.org/wiki/Digital_evidence
http://en.wikipedia.org/wiki/Demonstrative_evidence
http://en.wikipedia.org/wiki/Real_evidence
http://en.wikipedia.org/wiki/Chain_of_custody

QUESTION 9

To understand the 'whys' in crime, many times it is necessary to understand MOM. Which of the following is not a component of MOM?

A. Opportunities

B. Methods

C. Motivation

D. Means

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: To understand the whys in crime, many times it is necessary to understand the Motivations, Opportunities, and Means (MOM). Motivations are the who and why of a crime. Opportunities are the where and when of a crime, and Means pertains to the capabilities a criminal would need to be successful. Methods is not a component of MOM.

QUESTION 10
In the statement below, fill in the blank:
Law enforcement agencies must get a warrant to search and seize an individual's property, as stated in the Amendment.

A. First.

B. Second.

C. Third.

D. Fourth.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The Fourth Amendment does not apply to a seizure or an arrest by private citizens. Search and seizure activities can get tricky depending on what is being searched for and where. For example, American citizens are protected by the Fourth Amendment against unlawful search and seizure, so law enforcement agencies must have probable cause and request a search warrant from a judge or court before conducting such a search. The actual search can only take place in the areas outlined by the warrant. The Fourth Amendment does not apply to actions by private citizens unless they are acting as police agents. So, for example, if Kristy's boss warned all employees that the management could remove files from their computers at any time, and her boss was not a police officer or acting as a police agent, she could not successfully claim that her Fourth Amendment rights were violated. Kristy's boss may have violated some specific privacy laws, but he did not violate Kristy's Fourth Amendment rights.
In some circumstances, a law enforcement agent may seize evidence that is not included in the warrant, such as if the suspect tries to destroy the evidence. In other words, if there is an impending possibility that evidence might be destroyed, law enforcement may quickly seize the evidence to prevent its destruction. This is referred to as exigent circumstances, and a judge will later decide whether the seizure was proper and legal before allowing the evidence to be admitted. For example, if a police officer had a search warrant that allowed him to search a suspect's living room but no other rooms, and then he saw the suspect dumping cocaine down the toilet, the police officer could seize the cocaine even though it was in a room not covered under his search warrant. After evidence is gathered, the chain of custody needs to be enacted and enforced to make sure the evidence's integrity is not compromised.
All other choices were only detractors.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 1057). McGraw-Hill.
Kindle Edition.

QUESTION 11
Controls are implemented to:

A. eliminate risk and reduce the potential for loss

B. mitigate risk and eliminate the potential for loss

C. mitigate risk and reduce the potential for loss

D. eliminate risk and eliminate the potential for loss

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Controls are implemented to mitigate risk and reduce the potential for loss. Preventive controls are put in place to inhibit harmful occurrences; detective controls are established to discover harmful occurrences; corrective controls are used to restore systems that are victims of harmful attacks.
It is not feasible and possible to eliminate all risks and the potential for loss as risk/threats are constantly changing.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 32.

QUESTION 12
What can be described as a measure of the magnitude of loss or impact on the value of an asset?

A. Probability
B. Exposure factor
C. Vulnerability
D. Threat

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The exposure factor is a measure of the magnitude of loss or impact on the value of an asset.
The probability is the chance or likelihood, in a finite sample, that an event will occur or that a specific loss value may be attained should the event occur. A vulnerability is the absence or weakness of a risk-reducing safeguard. A threat is event, the occurrence of which could have an undesired impact. Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 3, August 1999.

QUESTION 13
Computer security should be first and foremost which of the following:

A. Cover all identified risks
B. Be cost-effective.
C. Be examined in both monetary and non-monetary terms.
D. Be proportionate to the value of IT systems.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Computer security should be first and foremost cost-effective. As for any organization, there is a need to measure their cost-effectiveness, to justify budget usage and provide supportive arguments for their next budget claim. But organizations often have difficulties to accurately measure the effectiveness and the cost of their information security activities.
The classical financial approach for ROI calculation is not particularly appropriate for measuring security-related initiatives: Security is not generally an investment that results in a profit. Security is more about loss prevention. In other terms, when you invest in security, you don't expect benefits; you expect to reduce the risks threatening your assets. The concept of the ROI calculation applies to every investment. Security is no exception. Executive decision-makers want to know the impact security is having on the bottom line. In order to know how much they should spend on security, they need to know how much is the lack of security costing to the business and what
are the most cost-effective solutions.
Applied to security, a Return On Security Investment (ROSI) calculation can provide quantitative answers to

essential financial questions:
Is an organization paying too much for its security?
What financial impact on productivity could have lack of security? When is the security investment enough?
Is this security product/organisation beneficial?
The following are other concerns about computer security but not the first and foremost:
The costs and benefits of security should be carefully examined in both monetary and nonmonetary terms to ensure that the cost of controls does not exceed expected benefits. Security should be appropriate and proportionate to the value of and degree of reliance on the IT systems and to the severity, probability, and extent of potential harm. Requirements for security vary, depending upon the particular IT system. Therefore it does not make sense for computer security to cover all identified risks when the cost of the measures exceeds the value of the systems they are protecting.
Reference(s) used for this question:
SWANSON, Marianne & GUTTMAN, Barbara, National Institute of Standards and Technology (NIST), NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996 (page 6).
and
http://www.enisa.europa.eu/activities/cert/other-work/introduction-to-return-on-security-investment

QUESTION 14
Which of the following best allows risk management results to be used knowledgeably?

A. A vulnerability analysis
B. A likelihood assessment
C. An uncertainty analysis
D. A threat identification

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Risk management consists of two primary and one underlying activity; risk assessment and risk mitigation are the primary activities and uncertainty analysis is the underlying one. After having performed risk assessment and mitigation, an uncertainty analysis should be performed. Risk management must often rely on speculation, best guesses, incomplete data, and many unproven assumptions. A documented uncertainty analysis allows the risk management results to be used knowledgeably. A vulnerability analysis, likelihood assessment and threat identification are all parts of the collection and analysis of data part of the risk assessment, one of the primary activities of risk management.
Source: SWANSON, Marianne & GUTTMAN, Barbara, National Institute of Standards and Technology (NIST), NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996 (pages 19-21).

QUESTION 15
What can be best defined as the examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment?

A. Risk management
B. Risk analysis
C. Threat analysis
D. Due diligence

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Threat analysis is the examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment.
The following answers are incorrect:

Risk analysis is the process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact.
Risk analysis is synonymous with risk assessment and part of risk management, which is the ongoing process of assessing the risk to mission/business as part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate, cost-effective controls to achieve and maintain an acceptable level or risk. Due Diligence is identifying possible risks that could affect a company based on best practices and standards.
Reference(s) used for this question:
STONEBURNER, Gary & al, National Institute of Standards and Technology (NIST), NIST Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001 (page B-3).

QUESTION 16
The first step in the implementation of the contingency plan is to perform:

A. A firmware backup
B. A data backup
C. An operating systems software backup
D. An application software backup

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: A data backup is the first step in contingency planning. Without data, there is nothing to process. "No backup, no recovery".
Backup for hardware should be taken care of next.
Formal arrangements must be made for alternate processing capability in case the need should arise.
Operating systems and application software should be taken care of afterwards. Source: VALLABHANENI, S. Rao, CISSP Examination Textbooks, Volume 2: Practice, SRV Professional Publications, 2002, Chapter 8, Business Continuity Planning & Disaster Recovery Planning (page 506).

QUESTION 17
The MOST common threat that impacts a business's ability to function normally is:

A. Power Outage
B. Water Damage
C. Severe Weather
D. Labor Strike

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The MOST common threat that impacts a business's ability to function normally is power. Power interruption cause more business interruption than any other type of event. The second most common threat is Water such as flood, water damage from broken pipe, leaky roof, etc...
Threats will be discovered while doing your Threats and Risk Assessments (TRA). There are three elements of risks: threats, assets, and mitigating factors (countermeasures, safeguards, controls).
A threat is an event or situation that if it occured would affect your business and may even prevent it from functioning normally or in some case functioning at all. Evaluation of threats is done by looking at Likelihood and Impact of possible threat. Safeguards, countermeasures, and controls would be used to bring the threat level down to an acceptable level.
Other common events that can impact a company are:
Weather, cable cuts, fires, labor disputes, transportation mishaps, hardware failure, chemical spills, sabotage.

The Official ISC2 Guide to the CISSP CBK, Second Edition, Page 275-276

QUESTION 18
Failure of a contingency plan is usually:

A. A technical failure.
B. A management failure.
C. Because of a lack of awareness.
D. Because of a lack of training.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Failure of a contingency plan is usually management failure to exhibit ongoing interest and concern about the BCP/DRP effort, and to provide financial and other resources as needed. Lack of management support will result in a lack awareness and training. Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 9: Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) (page 163).

QUESTION 19
Within the legal domain what rule is concerned with the legality of how the evidence was gathered ?

A. Exclusionary rule
B. Best evidence rule
C. Hearsay rule
D. Investigation rule

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The exclusionary rule mentions that evidence must be gathered legally or it can't be used.
The principle based on federal Constitutional Law that evidence illegally seized by law enforcement officers in violation of a suspect's right to be free from unreasonable searches and seizures cannot be used against the suspect in a criminal prosecution. The exclusionary rule is designed to exclude evidence obtained in violation of a criminal defendant's Fourth Amendment rights. The Fourth Amendment protects against unreasonable searches and seizures by law enforcement personnel. If the search of a criminal suspect is unreasonable, the evidence obtained in the search will be excluded from trial. The exclusionary rule is a court-made rule. This means that it was created not in statutes passed by legislative bodies but rather by the U.S. Supreme Court. The exclusionary rule applies in federal courts by virtue of the Fourth Amendment. The Court has ruled that it applies in state courts although the due process clause of the Fourteenth Amendment.(The Bill of Rights--the first ten amendments-- applies to actions by the federal government. The Fourteenth Amendment, the Court has held, makes most of the protections in the Bill of Rights applicable to actions by the states.)
The exclusionary rule has been in existence since the early 1900s. Before the rule was fashioned, any evidence was admissible in a criminal trial if the judge found the evidence to be relevant. The manner in which the evidence had been seized was not an issue. This began to change in 1914, when the U.S. Supreme Court devised a way to enforce the Fourth Amendment. In Weeks v. United States, 232 U.S. 383, 34 S. Ct. 341, 58 L. Ed. 652 (1914), a federal agent had conducted a warrantless search for evidence of gambling at the home of Fremont Weeks. The evidence seized in the search was used at trial, and Weeks was convicted. On appeal, the Court held that the Fourth Amendment barred the use of evidence secured through a warrantless search. Weeks's conviction was reversed, and thus was born the exclusionary rule. The best evidence rule concerns limiting potential for alteration. The best evidence rule is a common law rule of evidence which can be traced back at least as far as the 18th century. In Omychund v Barker (1745) 1 Atk, 21, 49; 26 ER 15, 33, Lord Harwicke stated that no evidence was admissible unless it was "the best that the nature of the case will allow". The general rule is that secondary evidence, such as a copy or facsimile, will be not admissible if an original document exists, and is not unavailable due to destruction or other circumstances indicating unavailability.
The rationale for the best evidence rule can be understood from the context in which it arose: in the eighteenth

century a copy was usually made by hand by a clerk (or even a litigant). The best evidence rule was predicated on the assumption that, if the original was not produced, there was a significant chance of error or fraud in relying on such a copy. The hearsay rule concerns computer-generated evidence, which is considered second-hand evidence.
Hearsay is information gathered by one person from another concerning some event, condition, or thing of which the first person had no direct experience. When submitted as evidence, such statements are called hearsay evidence. As a legal term, "hearsay" can also have the narrower meaning of the use of such information as evidence to prove the truth of what is asserted. Such use of "hearsay evidence" in court is generally not allowed. This prohibition is called the hearsay rule.
For example, a witness says "Susan told me Tom was in town". Since the witness did not see Tom in town, the statement would be hearsay evidence to the fact that Tom was in town, and not admissible. However, it would be admissible as evidence that Susan said Tom was in town, and on the issue of her knowledge of whether he was in town. Hearsay evidence has many exception rules. For the purpose of the exam you must be familiar with the business records exception rule to the Hearsay Evidence. The business records created during the ordinary course of business are considered reliable and can usually be brought in under this exception if the proper foundation is laid when the records are introduced into evidence. Depending on which jurisdiction the case is in, either the records custodian or someone with knowledge of the records must lay a foundation for the records. Logs that are collected as part of a document business process being carried at regular interval would fall under this exception. They could be presented in court and not be considered Hearsay.
Investigation rule is a detractor.
Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 9.
and
The FREE Online Law Dictionary at: http://legaldictionary.
thefreedictionary.com/Exclusionary+Rule
and
Wikipedia has a nice article on this subject at: http://en.wikipedia.org/wiki/Exclusionary_rule and http://en.wikipedia.org/wiki/Hearsay_in_United_States_law#Hearsay_exceptions

QUESTION 20
Computer-generated evidence is considered:

A. Best evidence
B. Second hand evidence
C. Demonstrative evidence
D. Direct evidence

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Computer-generated evidence normally falls under the category of hearsay evidence, or second-hand evidence, because it cannot be proven accurate and reliable. Under the U.S. Federal Rules of Evidence, hearsay evidence is generally not admissible in court. Best evidence is original or primary evidence rather than a copy or duplicate of the evidence. It does not apply to computer-generated evidence. Direct evidence is oral testimony by witness. Demonstrative evidence are used to aid the jury (models, illustrations, charts). Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 9: Law, Investigation, and Ethics (page 310).
And: ROTHKE, Ben, CISSP CBK Review presentation on domain 9.

QUESTION 21
Which of the following would be MOST important to guarantee that the computer evidence will be admissible in court?

A. It must prove a fact that is immaterial to the case.
B. Its reliability must be proven.
C. The process for producing it must be documented and repeatable.
D. The chain of custody of the evidence must show who collected, secured, controlled, handled, transported

the evidence, and that it was not tampered with.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: It has to be material, relevant and reliable, and the chain of custody must be maintained, it is unlikely that it will be admissible in court if it has been tampered with.
The following answers are incorrect:
It must prove a fact that is immaterial to the case. Is incorrect because evidence must be relevant.
If it is immaterial then it is not relevant.
Its reliability must be proven. Is incorrect because it is not the best answer. While evidence must be relevant if the chain of custody cannot be verified, then the evidence could lose it's credibility because there is no proof that the evidence was not tampered with. So, the correct answer above is the BEST answer.
The process for producing it must be documented and repeatable. Is incorrect because just because the process is documented and repeatable does not mean that it will be the same. This amounts to Corroborative Evidence that may help to support a case.

QUESTION 22
Which of the following would best describe secondary evidence?

A. Oral testimony by a non-expert witness
B. Oral testimony by an expert witness
C. A copy of a piece of evidence
D. Evidence that proves a specific act

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Secondary evidence is defined as a copy of evidence or oral description of its contents. It is considered not as reliable as best evidence. Evidence that proves or disproves a specific act through oral testimony based on information gathered through he witness's five senses is considered direct evidence. The fact that testimony is given by an expert only affects the witness's ability to offer an opinion instead of only testifying of the facts. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 9: Law, Investigation, and Ethics (page 310).

QUESTION 23
Why would a memory dump be admissible as evidence in court?

A. Because it is used to demonstrate the truth of the contents.
B. Because it is used to identify the state of the system.
C. Because the state of the memory cannot be used as evidence.
D. Because of the exclusionary rule.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: A memory dump can be admitted as evidence if it acts merely as a statement of fact. A system dump is not considered hearsay because it is used to identify the state of the system, not the truth of the contents. The exclusionary rule mentions that evidence must be gathered legally or it can't be used. This choice is a distracter. Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 10: Law, Investigation, and Ethics (page 187).

QUESTION 24

Which type of attack would a competitive intelligence attack best classify as?

A. Business attack
B. Intelligence attack
C. Financial attack
D. Grudge attack

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Business attacks concern information loss through competitive intelligence gathering and computer-related attacks. These attacks can be very costly due the loss of trade secrets and reputation. Intelligence attacks are aimed at sensitive military and law enforcement files containing military data and investigation reports.
Financial attacks are concerned with frauds to banks and large corporations. Grudge attacks are targeted at individuals and companies who have done something that the attacker doesn't like.
The CISSP for Dummies book has nice coverage of the different types of attacks, here is an extract:
Terrorism Attacks
Terrorism exists at many levels on the Internet. In April 2001, during a period of tense relations between China and the U.S. (resulting from the crash landing of a U.S. Navy reconnaissance plane on Hainan Island), Chinese hackers (cyberterrorists) launched a major effort to disrupt critical U.S. infrastructure, which included U.S. government and military systems. Following the terrorist attacks against the U.S. on September 11, 2001, the general public became painfully aware of the extent of terrorism on the Internet. Terrorist organizations and cells are using online capabilities to coordinate attacks, transfer funds, harm international commerce, disrupt critical systems, disseminate propaganda, and gain useful information about developing techniques and instruments of terror, including nuclear , biological, and chemical weapons.
Military and intelligence attacks
Military and intelligence attacks are perpetrated by criminals, traitors, or foreign intelligence agents seeking classified law enforcement or military information. Such attacks may also be carried out by governments during times of war and conflict.
Financial attacks
Banks, large corporations, and e-commerce sites are the targets of financial attacks, all of which are motivated by greed. Financial attacks may seek to steal or embezzle funds, gain access to online financial information, extort individuals or businesses, or obtain the personal credit card numbers of customers.
Business attacks
Businesses are becoming the targets of more and more computer and Internet attacks. These attacks include competitive intelligence gathering, denial of service, and other computer- related attacks. Businesses are often targeted for several reasons including Lack of expertise: Despite heightened security awareness, a shortage of qualified security professionals still exists, particularly in private enterprise. Lack of resources: Businesses often lack the resources to prevent, or even detect, attacks against their systems.
Lack of reporting or prosecution : Because of public relations concerns and the inability to prosecute computer criminals due to either a lack of evidence or a lack of properly handled evidence, the majority of business attacks still go unreported. The cost to businesses can be significant, including loss of trade secrets or proprietary information, loss of revenue, and loss of reputation.
Grudge attacks
Grudge attacks are targeted at individuals or businesses and are motivated by a desire to take revenge against a person or organization. A disgruntled employee, for example, may steal trade secrets, delete valuable data, or plant a logic bomb in a critical system or application. Fortunately, these attacks (at least in the case of a disgruntled employee) can be easier to prevent or prosecute than many other types of attacks because:
The attacker is often known to the victim.
The attack has a visible impact that produces a viable evidence trail. Most businesses (already sensitive to the possibility of wrongful termination suits) have wellestablished termination procedures
"Fun" attacks
"Fun" attacks are perpetrated by thrill seekers and script kiddies who are motivated by curiosity or excitement. Although these attackers may not intend to do any harm or use any of the information that they access, they're still dangerous and their activities are still illegal. These attacks can also be relatively easy to detect and

prosecute. Because the perpetrators are often script kiddies or otherwise inexperienced hackers, they may not know how to cover their tracks effectively.
Also, because no real harm is normally done nor intended against the system, it may be tempting (although ill advised) for a business to prosecute the individual and put a positive public relations spin on the incident. You've seen the film at 11: "We quickly detected the attack, prevented any harm to our network, and prosecuted the responsible individual; our security is unbreakable !" Such action, however, will likely motivate others to launch a more serious and concerted grudge attack against the business.
Many computer criminals in this category only seek notoriety. Although it's one thing to brag to a small circle of friends about defacing a public Web site, the wily hacker who appears on CNN reaches the next level of hacker celebrity-dom. These twisted individuals want to be caught to revel in their 15 minutes of fame.

ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 10: Law, Investigation, and Ethics (page 187) and
CISSP Professional Study Guide by James Michael Stewart, Ed Tittel, Mike Chapple, page 607- and
CISSP for Dummies, Miller L. H. and Gregory P. H. ISBN: 0470537914, page 309-311

QUESTION 25
Which of the following is an advantage of a qualitative over a quantitative risk analysis?

A. It prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities.
B. It provides specific quantifiable measurements of the magnitude of the impacts.
C. It makes a cost-benefit analysis of recommended controls easier.
D. It can easily be automated.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The main advantage of the qualitative impact analysis is that it prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities. It does not provide specific quantifiable measurements of the magnitude of the impacts, therefore making a cost-analysis of any recommended controls difficult. Since it involves a consensus of export and some guesswork based on the experience of Subject Matter Experts (SME's), it can not be easily automated.
Reference used for this question:
STONEBURNER, Gary et al., NIST Special publication 800-30, Risk management Guide for Information Technology Systems, 2001 (page 23).

QUESTION 26
Which of the following questions is less likely to help in assessing an organization's contingency planning controls?

A. Is damaged media stored and/or destroyed?
B. Are the backup storage site and alternate site geographically far enough from the primary site?
C. Is there an up-to-date copy of the plan stored securely off-site?
D. Is the location of stored backups identified?

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Contingency planning involves more than planning for a move offsite after a disaster destroys a facility.
It also addresses how to keep an organization's critical functions operating in the event of disruptions, large and small.
Handling of damaged media is an operational task related to regular production and is not specific to contingency planning.
Source: SWANSON, Marianne, NIST Special Publication 800-26, Security Self-Assessment Guide for

Information Technology Systems, November 2001 (Pages A-27 to A-28).

QUESTION 27
When a possible intrusion into your organization's information system has been detected, which of the following actions should be performed first?

A. Eliminate all means of intruder access.
B. Contain the intrusion.
C. Determine to what extent systems and data are compromised.
D. Communicate with relevant parties.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Once an intrusion into your organization's information system has been detected, the first action that needs to be performed is determining to what extent systems and data are compromised (if they really are), and then take action. This is the good old saying: "Do not cry wolf until you know there is a wolf for sure" Sometimes it smells like a wolf, it looks like a wolf, but it may not be a wolf. Technical problems or bad hardware might cause problems that looks like an intrusion even thou it might not be. You must make sure that a crime has in fact been committed before implementing your reaction plan. Information, as collected and interpreted through analysis, is key to your decisions and actions while executing response procedures. This first analysis will provide information such as what attacks were used, what systems and data were accessed by the intruder, what the intruder did after obtaining access and what the intruder is currently doing (if the intrusion has not been contained).
The next step is to communicate with relevant parties who need to be made aware of the intrusion in a timely manner so they can fulfil their responsibilities. Step three is concerned with collecting and protecting all information about the compromised systems and causes of the intrusion. It must be carefully collected, labelled, catalogued, and securely stored.
Containing the intrusion, where tactical actions are performed to stop the intruder's access, limit the extent of the intrusion, and prevent the intruder from causing further damage, comes next. Since it is more a long-term goal, eliminating all means of intruder access can only be achieved last, by implementing an ongoing security improvement process.
Reference used for this question:
ALLEN, Julia H., The CertKingdom to System and Network Security Practices, Addison-Wesley, 2001, Chapter 7: Responding to Intrusions (pages 271-289).

QUESTION 28
When first analyzing an intrusion that has just been detected and confirming that it is a true positive, which of the following actions should be done as a first step if you wish to prosecute the attacker in court?

A. Back up the compromised systems.
B. Identify the attacks used to gain access.
C. Capture and record system information.
D. Isolate the compromised systems.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: When an intrusion has been detected and confirmed, if you wish to prosecute the attacker in court, the following actions should be performed in the following order:
Capture and record system information and evidence that may be lost, modified, or not captured during the execution of a backup procedure. Start with the most volative memory areas first. Make at least two full backups of the compromised systems, using hardware-write-protectable or write-once media. A first backup may be used to re-install the compromised system for further analysis and the second one should be preserved in a secure location to preserve the chain of custody of evidence.

Isolate the compromised systems.
Search for signs of intrusions on other systems.
Examine logs in order to gather more information and better identify other systems to which the intruder might have gained access.
Search through logs of compromised systems for information that would reveal the kind of attacks used to gain access.
Identify what the intruder did, for example by analyzing various log files, comparing checksums of known, trusted files to those on the compromised machine and by using other intrusion analysis tools.
Regardless of the exact steps being followed, if you wish to prosecute in a court of law it means you MUST capture the evidence as a first step before it could be lost or contaminated. You always start with the most volatile evidence first.
NOTE:
I have received feedback saying that some other steps may be done such as Disconnecting the system from the network or shutting down the system. This is true. However, those are not choices listed within the 4 choices attached to this question, you MUST avoid changing the question. You must stick to the four choices presented and pick which one is the best out of the four presented.
In real life, Forensic is not always black or white. There are many shades of grey. In real life you would have to consult your system policy (if you have one), get your Computer Incident team involved, and talk to your forensic expert and then decide what is the best course of action.
Reference(s) Used for this question:
http://www.newyorkcomputerforensics.com/learn/forensics_process.php and
ALLEN, Julia H., The CertKingdom to System and Network Security Practices, Addison-Wesley, 2001, Chapter 7: Responding to Intrusions (pages 273-277).

QUESTION 29
In order to be able to successfully prosecute an intruder:

A. A point of contact should be designated to be responsible for communicating with law enforcement and other external agencies.
B. A proper chain of custody of evidence has to be preserved.
C. Collection of evidence has to be done following predefined procedures.
D. Whenever possible, analyze a replica of the compromised resource, not the original, thereby avoiding inadvertently tamping with evidence.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: If you intend on prosecuting an intruder, evidence has to be collected in a lawful manner and, most importantly, protected through a secure chain-of-custody procedure that tracks who has been involved in handling the evidence and where it has been stored. All other choices are all important points, but not the best answer, since no prosecution is possible without a proper, provable chain of custody of evidence.
Source: ALLEN, Julia H., The CertKingdom to System and Network Security Practices, Addison- Wesley, 2001, Chapter 7: Responding to Intrusions (pages 282-285).

QUESTION 30
When referring to a computer crime investigation, which of the following would be the MOST important step required in order to preserve and maintain a proper chain of custody of evidence:

A. Evidence has to be collected in accordance with all laws and all legal regulations.
B. Law enforcement officials should be contacted for advice on how and when to collect critical information.
C. Verifiable documentation indicating the who, what, when, where, and how the evidence was handled should be available.
D. Log files containing information regarding an intrusion are retained for at least as long as normal business records, and longer in the case of an ongoing investigation.

Correct Answer: C

Explanation

Explanation/Reference:
Explanation: Two concepts that are at the heart of dealing effectively with digital/electronic evidence, or any evidence for that matter, are the chain of custody and authenticity/integrity. The chain of custody refers to the who, what, when, where, and how the evidence was handled--from its identification through its entire life cycle, which ends with destruction or permanent archiving.
Any break in this chain can cast doubt on the integrity of the evidence and on the professionalism of those directly involved in either the investigation or the collection and handling of the evidence. The chain of custody requires following a formal process that is well documented and forms part of a standard operating procedure that is used in all cases, no exceptions.
The following are incorrect answers:
Evidence has to be collected in accordance with all laws and legal regulations. Evidence would have to be collected in accordance with applicable laws and regulations but not necessarily with ALL laws and regulations. Only laws and regulations that applies would be followed. Law enforcement officials should be contacted for advice on how and when to collect critical information. It seems you failed to do your homework, once you have an incident it is a bit late to do this. Proper crime investigation as well as incident response is all about being prepared ahead of time. Obviously, you are improvising if you need to call law enforcement to find out what to do. It is a great way of contaminating your evidence by mistake if you don't have a well documented processs with clear procedures that needs to be followed. Log files containing information regarding an intrusion are retained for at least as long as normal business records, and longer in the case of an ongoing investigation. Specific legal requirements exists for log retention and they are not the same as normal business records. Laws such as Basel, HIPPAA, SOX, and others has specific requirements.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 23465-23470). Auerbach Publications. Kindle Edition.
and
ALLEN, Julia H., The CertKingdom to System and Network Security Practices, Addison-Wesley, 2001, Chapter 7: Responding to Intrusions (pages 282-285).

QUESTION 31
When should a post-mortem review meeting be held after an intrusion has been properly taken care of?

A. Within the first three months after the investigation of the intrusion is completed.
B. Within the first week after prosecution of intruders have taken place, whether successful or not.
C. Within the first month after the investigation of the intrusion is completed.
D. Within the first week of completing the investigation of the intrusion.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: A post-mortem review meeting should be held with all involved parties within three to five working days of completing the investigation of the intrusion. Otherwise, participants are likely to forget critical information. Even if it enabled an organization to validate the correctness of its chain of custody of evidence, it would not make sense to wait until prosecution is complete because it would take too much time and many cases of intrusion never get to court anyway. Source: ALLEN, Julia H., The CertKingdom to System and Network Security Practices, Addison- Wesley, 2001, Chapter 7: Responding to Intrusions (page 297).

QUESTION 32
What can be defined as an event that could cause harm to the information systems?

A. A risk
B. A threat
C. A vulnerability
D. A weakness

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: A threat is an event or activity that has the potential to cause harm to the information systems. A risk is the probability that a threat will materialize. A vulnerability, or weakness, is a lack of a safeguard, which may be exploited by a threat, causing harm to the information systems. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 1: Access Control Systems (page 32).

QUESTION 33
Most access violations are:

A. Accidental
B. Caused by internal hackers
C. Caused by external hackers
D. Related to Internet

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The most likely source of exposure is from the uninformed, accidental or unknowing person, although the greatest impact may be from those with malicious or fraudulent intent. Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 4: Protection of Information Assets (page 192).

QUESTION 34
A business continuity plan is an example of which of the following?

A. Corrective control
B. Detective control
C. Preventive control
D. Compensating control

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Business Continuity Plans are designed to minimize the damage done by the event, and facilitate rapid restoration of the organization to its full operational capacity. They are for use "after the fact", thus are examples of corrective controls.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 273).
and
Conrad, Eric; Misenar, Seth; Feldman, Joshua (2012-09-01). CISSP Study Guide (Kindle Location 8069). Elsevier Science (reference). Kindle Edition.
and

QUESTION 35
When preparing a business continuity plan, who of the following is responsible for identifying and prioritizing time-critical systems?

A. Executive management staff

B. Senior business unit management

C. BCP committee

D. Functional business units

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Many elements of a BCP will address senior management, such as the statement of importance and priorities, the statement of organizational responsibility, and the statement of urgency and timing. Executive management staff initiates the project, gives final approval and gives ongoing support. The BCP committee directs the planning, implementation, and tests processes whereas functional business units participate in implementation and testing. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 275).

QUESTION 36
Which of the following statements pertaining to disaster recovery planning is incorrect?

A. Every organization must have a disaster recovery plan

B. A disaster recovery plan contains actions to be taken before, during and after a disruptive event.

C. The major goal of disaster recovery planning is to provide an organized way to make decisions if a disruptive event occurs.

D. A disaster recovery plan should cover return from alternate facilities to primary facilities.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: It is possible that an organization may not need a disaster recovery plan. An organization may not have any critical processing areas or system and they would be able to withstand lengthy interruptions. Remember that DRP is related to systems needed to support your most critical business functions. The DRP plan covers actions to be taken when a disaster occur but DRP PLANNING which is the keywork in the question would also include steps that happen before you use the plan such as development of the plan, training, drills, logistics, and a lot more. To be effective, the plan would certainly cover before, during, and after the disaster actions. It may take you a couple years to develop a plan for a medium size company, there is a lot that has to happen before the plan would be actually used in a real disaster scenario. Plan for the worst and hope for the best.
All other statements are true.
NOTE FROM CLEMENT:
Below is a great article on who legally needs a plan which is very much in line with this question. Does EVERY company needs a plan? The legal answer is NO. Some companies, industries, will be required according to laws or regulations to have a plan. A blank statement saying: All companies MUST have a plan would not be accurate. The article below is specific to the USA but similar laws will exist in many other countries.
Some companies such as utilities, power, etc... might also need plan if they have been defined as Critical Infrastructure by the government. The legal side of IT is always very complex and varies in different countries. Always talk to your lawyer to ensure you follow the law of the land :-) Read the details below:
So Who, Legally, MUST Plan?
With the caveats above, let's cover a few of the common laws where there is a duty to have a disaster recovery plan. I will try to include the basis for that requirement, where there is an implied mandate to do so, and what the difference is between the two Banks and Financial Institutions MUST Have a Plan
The Federal Financial Institutions Examination Council (Council) was established on March 10, 1979, pursuant to Title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978 (FIRA), Public Law 95-630. In 1989, Title XI of the Financial Institutions Reform, Recovery and Enforcement Act of 1989 (FIRREA) established the Examination Council (the Council). The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation

(FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS); and to make recommendations to promote uniformity in the supervision of financial institutions. In other words, every bank, savings and loan, credit union, and other financial institution is governed by the principles adopted by the Council. In March of 2003, the Council released its Business Continuity Planning handbook designed to provide guidance and examination procedures for examiners in evaluating financial institution and service provider risk-management processes.

Stockbrokers MUST Have a Plan

The National Association of Securities Dealers (NASD) has adopted rules that require all its members to have business continuity plans. The NASD oversees the activities of more than 5,100 brokerage firms, approximately 130,800 branch offices and more than 658,770 registered securities representatives.

As of June 14, 2004, the rules apply to all NASD member firms. The requirements, which are specified in Rule 3510, begin with the following:

3510. Business Continuity Plans. (a) Each member must create and maintain a written business continuity plan identifying procedures relating to an emergency or significant business disruption. Such procedures must be reasonably designed to enable the member to meet its existing obligations to customers. In addition, such procedures must address the member's existing relationships with other broker-dealers and counter-parties. The business continuity plan must be made available promptly upon request to NASD staff.

NOTE:

The rules apply to every company that deals in securities, such as brokers, dealers, and their representatives, it does NOT apply to the listed companies themselves.

Electric Utilities WILL Need a Plan

The disaster recovery function relating to the electric utility grid is presently undergoing a change. Prior to 2005, the Federal Energy Regulatory Commission (FERC) could only coordinate volunteer efforts between utilities. This has changed with the adoption of Title XII of the Energy Policy Act of 2005 (16 U.S.C. 824o). That new law authorizes the FERC to create an Electric Reliability Organization (ERO).

The ERO will have the capability to adopt and enforce reliability standards for "all users, owners, and operators of the bulk power system" in the United States. At this time, FERC is in the process of finalizing the rules for the creation of the ERO. Once the ERO is created, it will begin the process of establishing reliability standards. It is very safe to assume that the ERO will adopt standards for service restoration and disaster recovery, particularly after such widespread disasters as Hurricane Katrina. Telecommunications Utilities SHOULD Have Plans, but MIGHT NOT Telecommunications utilities are governed on the federal level by the Federal Communications Commission (FCC) for interstate services and by state Public Utility Commissions (PUCs) for services within the state.

The FCC has created the Network Reliability and Interoperability Council (NRIC). The role of the NRIC is to develop recommendations for the FCC and the telecommunications industry to "insure [sic] optimal reliability, security, interoperability and interconnectivity of, and accessibility to, public communications networks and the internet." The NRIC members are senior representatives of providers and users of telecommunications services and products, including telecommunications carriers, the satellite, cable television, wireless and computer industries, trade associations, labor and consumer representatives, manufacturers, research organizations, and government-related organizations.

There is no explicit provision that we could find that says telecommunications carriers must have a Disaster Recovery Plan. As I have stated frequently in this series of articles on disaster recovery, however, telecommunications facilities are tempting targets for terrorism. I have not changed my mind in that regard and urge caution.

You might also want to consider what the liability of a telephone company is if it does have a disaster that causes loss to your organization. In three words: It's not much. The following is the statement used in most telephone company tariffs with regard to its liability:

The Telephone Company's liability, if any, for its gross negligence or willful misconduct is not limited by this tariff. With respect to any other claim or suit, by a customer or any others, for damages arising out of mistakes, omissions, interruptions, delays or errors, or defects in transmission occurring in the course of furnishing services hereunder, the Telephone Company's liability, if any, shall not exceed an amount equivalent to the proportionate charge to the customer for the period of service during which such mistake, omission, interruption, delay, error or defect in transmission or service occurs and continues. (Source, General Exchange Tariff for major carrier) All Health Care Providers WILL Need a Disaster Recovery Plan HIPAA is an acronym for the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, which amended the Internal Revenue Service Code of 1986. Also known as the Kennedy-Kassebaum Act, the Act includes a section, Title II, entitled Administrative Simplification, requiring "Improved efficiency in healthcare delivery by standardizing electronic data interchange, and protection of confidentiality and security of health data through setting and enforcing standards."

The legislation called upon the Department of Health and Human Services (HHS) to publish new rules that will ensure security standards protecting the confidentiality and integrity of "individually identifiable health information," past, present, or future. The final Security Rule was published by HHS on February 20, 2003 and provides for a uniform level of protection of all health information that is housed or transmitted electronically and that pertains to an individual.

The Security Rule requires covered entities to ensure the confidentiality, integrity, and availability of all electronic protected health information (ePHI) that the covered entity creates, receives, maintains, or transmits. It also requires entities to protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI, protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required by the Privacy Rule, and ensure compliance by their workforce.

Required safeguards include application of appropriate policies and procedures, safeguarding physical access to ePHI, and ensuring that technical security measures are in place to protect networks, computers and other electronic devices.

Companies with More than 10 Employees

The United States Department of Labor has adopted numerous rules and regulations in regard to workplace safety as part of the Occupational Safety and Health Act. For example, 29 USC 654 specifically requires:

(a) Each employer:

(1) shall furnish to each of his employees employment and a place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees;

(2) shall comply with occupational safety and health standards promulgated under this Act. (b) Each employee shall comply with occupational safety and health standards and all rules, regulations, and orders issued pursuant to this Act which are applicable to his own actions and conduct.

Other Considerations or Expensive Research question NO: s for Lawyers (Sorry, Eddie!) The Foreign Corrupt Practices Act of 1977

Internal Revenue Service (IRS) Law for Protecting Taxpayer Information Food and Drug Administration (FDA) Mandated Requirements Homeland Security and Terrorist Prevention

Pandemic (Bird Flu) Prevention

ISO 9000 Certification

Requirements for Radio and TV Broadcasters

Contract Obligations to Customers

Document Protection and Retention Laws

Personal Identity Theft...and MORE!

Suffice it to say you will need to check with your legal department for specific requirements in your business and industry!

I would like to thank my good friend, Eddie M. Pope, for his insightful contributions to this article, our upcoming book, and my ever-growing pool of lawyer jokes. If you want more information on the legal aspects of recovery planning, Eddie can be contacted at my company or via email at mailto:mempope@tellawcomlabs.com. (Eddie cannot, of course, give you legal advice, but he can point you in the right direction.)

I hope this article helps you better understand the complex realities of the legal reasons why we plan and wish you the best of luck

See original article at: http://www.informit.com/articles/article.aspx?p=777896 See another interesting article on the subject at:

http://www.informit.com/articles/article.aspx?p=677910&seqNum=1 References used for this question: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 281).

QUESTION 37

Which of the following statements do not apply to a hot site?

A. It is expensive.

B. There are cases of common overselling of processing capabilities by the service provider.

C. It provides a false sense of security.

D. It is accessible on a first come first serve basis. In case of large disaster it might not be accessible.

Correct Answer: C

Explanation

Explanation/Reference:
Explanation: Remember this is a NOT question. Hot sites do not provide a false sense of security since they are the best disaster recovery alternate for backup site that you rent. A Cold, Warm, and Hot site is always a rental place in the context of the CBK. This is definivily the best choices out of the rental options that exists. It is fully configured and can be activated in a very short period of time.
Cold and Warm sites, not hot sites, provide a false sense of security because you can never fully test your plan.
In reality, using a cold site will most likely make effective recovery impossible or could lead to business closure if it takes more than two weeks for recovery. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 284).

QUESTION 38
What can be defined as a batch process dumping backup data through communications lines to a server at an alternate location?

A. Remote journaling
B. Electronic vaulting
C. Data clustering
D. Database shadowing

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Electronic vaulting refers to the transfer of backup data to an off-site location. This is primarily a batch process of dumping backup data through communications lines to a server at an alternate location. Electronic vaulting is accomplished by backing up system data over a network. The backup location is usually at a separate geographical location known as the vault site. Vaulting can be used as a mirror or a backup mechanism using the standard incremental or differential backup cycle. Changes to the host system are sent to the vault server in real-time when the backup method is implemented as a mirror. If vaulting updates are recorded in real-time, then it will be necessary to perform regular backups at the off-site location to provide recovery services due to inadvertent or malicious alterations to user or system data.
The following are incorrect answers:
Remote journaling refers to the parallel processing of transactions to an alternate site (as opposed to a batch dump process). Journaling is a technique used by database management systems to provide redundancy for their transactions. When a transaction is completed, the database management system duplicates the journal entry at a remote location. The journal provides sufficient detail for the transaction to be replayed on the remote system. This provides for database recovery in the event that the database becomes corrupted or unavailable. Database shadowing uses the live processing of remote journaling, but creates even more redundancy by duplicating the database sets to multiple servers. There are also additional redundancy options available within application and database software platforms. For example, database shadowing may be used where a database management system updates records in multiple locations. This technique updates an entire copy of the database at a remote location. Data clustering refers to the classification of data into groups (clusters). Clustering may also be used, although it should not be confused with redundancy. In clustering, two or more "partners" are joined into the cluster and may all provide service at the same time. For example, in an activeactive pair, both systems may provide services at any time. In the case of a failure, the remaining partners may continue to provide service but at a decreased capacity. The following resource(s) were used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 20403-20407 and 20411-20414 and 20375-20377 and 20280- 20283). Auerbach Publications. Kindle Edition.

QUESTION 39
Which of the following is the most complete disaster recovery plan test type, to be performed after successfully completing the Parallel test?

A. Full Interruption test

B. Checklist test
C. Simulation test
D. Structured walk-through test

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The difference between this and the full-interruption test is that the primary production processing of the business does not stop; the test processing runs in parallel to the real processing. This is the most common type of disaster recovery plan testing. A checklist test is only considered a preliminary step to a real test. In a structured walk-through test, business unit management representatives meet to walk through the plan, ensuring it accurately reflects the organization's ability to recover successfully, at least on paper.
A simulation test is aimed at testing the ability of the personnel to respond to a simulated disaster, but not recovery process is actually performed.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 289).

QUESTION 40
Which of the following statements pertaining to disaster recovery is incorrect?

A. A recovery team's primary task is to get the pre-defined critical business functions at the alternate backup processing site.
B. A salvage team's task is to ensure that the primary site returns to normal processing conditions.
C. The disaster recovery plan should include how the company will return from the alternate site to the primary site.
D. When returning to the primary site, the most critical applications should be brought back first.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: It's interesting to note that the steps to resume normal processing operations will be different than the steps in the recovery plan; that is, the least critical work should be brought back first to the primary site.
My explanation:
at the point where the primary site is ready to receive operations again, less critical systems should be brought back first because one has to make sure that everything will be running smoothly at the primary site before returning critical systems, which are already operating normally at the recovery site.
This will limit the possible interruption of processing to a minimum for most critical systems, thus making it the best option.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 291).

QUESTION 41
If an employee's computer has been used by a fraudulent employee to commit a crime, the hard disk may be seized as evidence and once the investigation is complete it would follow the normal steps of the Evidence Life Cycle. In such case, the Evidence life cycle would not include which of the following steps listed below?

A. Acquisition collection and identification
B. Analysis
C. Storage, preservation, and transportation
D. Destruction

Correct Answer: D

Explanation

Explanation/Reference:
Explanation: Unless the evidence is illegal then it should be returned to owner, not destroyed. The Evidence Life Cycle starts with the discovery and collection of the evidence. It progresses through the following series of states until it is finally returned to the victim or owner:
· Acquisition collection and identification
· Analysis
· Storage, preservation, and transportation
· Presented in court
· Returned to victim (owner)
The Second edition of the ISC2 book says on page 529-530:
Identifying evidence: Correctly identifying the crime scene, evidence, and potential containers of evidence.
Collecting or acquiring evidence: Adhering to the criminalistic principles and ensuring that the contamination and the destruction of the scene are kept to a minimum. Using sound, repeatable, collection techniques that allow for the demonstration of the accuracy and integrity of evidence, or copies of evidence.
Examining or analyzing the evidence: Using sound scientific methods to determine the characteristics of the evidence, conducting comparison for individuation of evidence, and conducting event reconstruction.
Presentation of findings: Interpreting the output from the examination and analysis based on findings of fact and articulating these in a format appropriate for the intended audience (e.g., court brief, executive memo, report).
Note on returning the evidence to the Owner/Victim
The final destination of most types of evidence is back with its original owner. Some types of evidence, such as drugs or drug paraphernalia (i.e., contraband), are destroyed after the trial. Any evidence gathered during a search, although maintained by law enforcement, is legally under the control of the courts. And although a seized item may be yours and may even have your name on it, it might not be returned to you unless the suspect signs a release or after a hearing by the court. Unfortunately, many victims do not want to go to trial; they just want to get their property back.
Many investigations merely need the information on a disk to prove or disprove a fact in question; thus, there is no need to seize the entire system. Once a schematic of the system is drawn or photographed, the hard disk can be removed and then transported to a forensic lab for copying. Mirror copies of the suspect disk are obtained using forensic software and then one of those copies can be returned to the victim so that business operations can resume.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 9: Law, Investigation, and Ethics (page 309).
and
The Official Study Book, Second Edition, Page 529-230

QUESTION 42
Which of the following is a problem regarding computer investigation issues?

A. Information is tangible.
B. Evidence is easy to gather.
C. Computer-generated records are only considered secondary evidence, thus are not as reliable as best evidence.
D. In many instances, an expert or specialist is not required.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Because computer-generated records normally fall under the category of hearsay evidence because they cannot be proven accurate and reliable this can be a problem. Under the U.S. Federal Rules of Evidence, hearsay evidence is generally not admissible in court. This inadmissibility is known as the hearsay rule, although there are some exceptions for how, when, by whom and in what circumstances data was collected. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 9: Law, Investigation, and Ethics (page

310).
IMPORTANT NOTE:
For the purpose of the exam it is very important to remember the Business Record exemption to the Hearsay Rule. For example: if you create log files and review them on a regular basis as part of a business process, such files would be admissable in court and they would not be considered hearsay because they were made in the course of regular business and it is part of regular course of business to create such record.
Here is another quote from the HISM book:
Business Record Exemption to the Hearsay Rule
Federal Rules of Evidence 803(6) allow a court to admit a report or other business document made at or near the time by or from information transmitted by a person with knowledge, if kept in the course of regularly conducted business activity, and if it was the regular practice of that business activity to make the [report or document], all as shown by testimony of the custodian or other qualified witness, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness.
To meet Rule 803(6) the witness must:
· Have custody of the records in question on a regular basis. · Rely on those records in the regular course of business. · Know that they were prepared in the regular course of business. Audit trails meet the criteria if they are produced in the normal course of business. The process to produce the output will have to be proven to be reliable. If computer-generated evidence is used and admissible, the court may order disclosure of the details of the computer, logs, and maintenance records in respect to the system generating the printout, and then the defense may use that material to attack the reliability of the evidence. If the audit trails are not used orreviewed -- at least the exceptions (e.g., failed log-on attempts) -- in the regular course of business, they do not meet the criteria for admissibility.
Federal Rules of Evidence 1001(3) provide another exception to the hearsay rule. This rule allows a memory or disk dump to be admitted as evidence, even though it is not done in the regular course of business. This dump merely acts as statement of fact. System dumps (in binary or hexadecimal) are not hearsay because they are not being offered to prove the truth of the contents, but only the state of the computer.
BUSINESS RECORDS LAW EXAMPLE:
The business records law was enacted in 1931 (PA No. 56). For a document to be admissible under the statute, the proponent must show: (1) the document was made in the regular course of business; (2) it was the regular course of business to make the record; and (3) the record was made when the act, transaction, or event occurred, or shortly thereafter (State v. Vennard, 159 Conn. 385, 397 (1970); Mucci v. LeMonte, 157 Conn. 566, 570 (1969). The failure to establish any one of these essential elements renders the document inadmissible under the statute (McCahill v. Town and Country Associates, Ltd. , 185 Conn. 37 (1981); State v. Peary, 176 Conn. 170 (1978); Welles v. Fish Transport Co. , , 123 Conn. 49 (1937).
The statute expressly provides that the person who made the business entry does not have to be unavailable as a witness and the proponent does not have to call as a witness the person who made the record or show the person to be unavailable (State v. Jeustiniano, 172 Conn. 275 (1977).
The person offering the business records as evidence does not have to independently prove the trustworthiness of the record. But, there is no presumption that the record is accurate; the record's accuracy and weight are issues for the trier of fact (State v. Waterman, 7 Conn. App. 326 (1986); Handbook of Connecticut Evidence, Second Edition, § 11. 14. 3). http://search.cga.state.ct.us/dtsearch_lpa.asp?cmd=getdoc&DocId=16833&Index=I%3A%5Czinde x%5C1995&HitCount=0&hits=&hc=0&req=&Item=712

QUESTION 43
What is defined as inference of information from other, intermediate, relevant facts?

A. Secondary evidence
B. Conclusive evidence
C. Hearsay evidence
D. Circumstantial evidence

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Circumstantial evidence is defined as inference of information from other, intermediate, relevant facts. Secondary evidence is a copy of evidence or oral description of its contents. Conclusive evidence is incontrovertible and overrides all other evidence and hearsay evidence is evidence that is not based on

personal, first-hand knowledge of the witness, but was obtained from another source. Computer-generated records normally fall under the category of hearsay evidence.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 9: Law, Investigation, and Ethics (page 310).

QUESTION 44
Under the Business Exemption Rule to the hearsay evidence, which of the following exceptions would have no bearing on the inadmissibility of audit logs and audit trails in a court of law?

A. Records are collected during the regular conduct of business.
B. Records are collected by senior or executive management.
C. Records are collected at or near the time of occurrence of the act being investigated to generate automated reports.
D. You can prove no one could have changed the records/data/logs that were collected.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Hearsay evidence is not normally admissible in court unless it has firsthand evidence that can be used to prove the evidence's accuracy, trustworthiness, and reliability like a business person who generated the computer logs and collected them. It is important that this person generates and collects logs as a normal part of his business and not just this one time for court. It has to be a documented process that is carried out daily. The value of evidence depends upon the genuineness and competence of the source; therefore, since record collection is not an activity likely to be performed by senior or executive management, records collected by senior or executive management are not likely to be admissible in court. Hearsay evidence is usually not admissible in court unless it meets the Business Records Exemption rule to the Hearsay evidence.
· In certain instances computer records fall outside of the hearsay rule (e.g., business records exemption)
· Information relates to regular business activities
· Automatically computer generated data
· No human intervention
· Prove system was operating correctly
· Prove no one changed the data
If you have a documented business process and you make use of intrusion detection tools, log analysis tools, and you produce daily reports of activities, then the computer generated data might be admissible in court and would not be considered Hearsay Evidence.
Reference(s) used for this question:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 10: Law, Investigation, and Ethics (page 676).

QUESTION 45
Which of the following categories of hackers poses the greatest threat?

A. Disgruntled employees
B. Student hackers
C. Criminal hackers
D. Corporate spies

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: According to the authors, hackers fall in these categories, in increasing threat order:
security experts, students, underemployed adults, criminal hackers, corporate spies and disgruntled employees.
Disgruntled employees are the most dangerous security problem of all because they are most likely to have a good knowledge of the organization's IT systems and security measures. Source: STREBE, Matthew and

PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 2:
Hackers.

QUESTION 46
Which of the following best defines a Computer Security Incident Response Team (CSIRT)?

A. An organization that provides a secure channel for receiving reports about suspected security incidents.
B. An organization that ensures that security incidents are reported to the authorities.
C. An organization that coordinates and supports the response to security incidents.
D. An organization that disseminates incident-related information to its constituency and other involved parties.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: RFC 2828 (Internet Security Glossary) defines a Computer Security Incident Response Team (CSIRT) as an organization that coordinates and supports the response to security incidents that involves sites within a defined constituency. This is the proper definition for the CSIRT. To be considered a CSIRT, an organization must provide a secure channel for receiving reports about suspected security incidents, provide assistance to members of its constituency in handling the incidents and disseminate incident-related information to its constituency and other involved parties. Security-related incidents do not necessarily have to be reported to the authorities.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 47
Under the principle of culpable negligence, executives can be held liable for losses that result from computer system breaches if:

A. The company is not a multi-national company.
B. They have not exercised due care protecting computing resources.
C. They have failed to properly insure computer resources against loss.
D. The company does not prosecute the hacker that caused the breach.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Culpable negligence is defined as: Recklessly acting without reasonable caution and putting another person at risk of injury or death (or failing to do something with the same consequences)
Where a suspected security breach has been caused (through wilful intent or culpable negligence) disciplinary action may be sought in line with the appropriate misconduct guidelines for internal employees.
By not exercising Due Care and taking the proper actions, the executives would be liable for losses a company has suffered.
Reference(s) used for this question:
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.
and
http://www.thefreedictionary.com/culpable+negligence

QUESTION 48
The deliberate planting of apparent flaws in a system for the purpose of detecting attempted penetrations or confusing an intruder about which flaws to exploit is called:

A. alteration
B. investigation
C. entrapment

D. enticement.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Enticement deals with someone that is breaking the law. Entrapment encourages someone to commit a crime that the individual may or many have had no intention of committing. Enticement is not necessarily illegal but does raise ethical arguments and may not be admissible in court. Enticement lures someone toward some evidence (a honeypot would be a great example) after that individual has already committed a crime.
Entrapment is when you persuade someone to commit a crime when the person otherwise had no intention to commit a crime. Entrapment is committed by a law enforcement player where you get tricked into committing a crime for which you woud later on get arrested without knowing you rare committing such a scrime. It is illegal and unethical as well. All other choices were not applicable and only detractors.

TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.
and
CISSP Study Guide (Conrad, Misenar, Feldman). Elsevier. 2010. p. 428 and
http://www.dummies.com/how-to/content/security-certification-computer-forensics-and-inci.html

QUESTION 49
Which element must computer evidence have to be admissible in court?

A. It must be relevant.
B. It must be annotated.
C. It must be printed.
D. It must contain source code.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 50
For which areas of the enterprise are business continuity plans required?

A. All areas of the enterprise.
B. The financial and information processing areas of the enterprise.
C. The operating areas of the enterprise.
D. The marketing, finance, and information processing areas.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 51
Which of the following will a Business Impact Analysis NOT identify?

A. Areas that would suffer the greatest financial or operational loss in the event of a disaster.
B. Systems critical to the survival of the enterprise.
C. The names of individuals to be contacted during a disaster.

D. The outage time that can be tolerated by the enterprise as a result of a disaster.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 52
What is a hot-site facility?

A. A site with pre-installed computers, raised flooring, air conditioning, telecommunications and networking equipment, and UPS.
B. A site in which space is reserved with pre-installed wiring and raised floors.
C. A site with raised flooring, air conditioning, telecommunications, and networking equipment, and UPS.
D. A site with ready made work space with telecommunications equipment, LANs, PCs, and terminals for work groups.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 53
Which of the following best describes remote journaling?

A. Send hourly tapes containing transactions off-site.
B. Send daily tapes containing transactions off-site.
C. Real-time capture of transactions to multiple storage devices.
D. Real time transmission of copies of the entries in the journal of transactions to an alternate site.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Remote Journaling is a technology to facilitate sending copies of the journal of transaction entries from a production system to a secondary system in realtime. The remote nature of such a connection is predicated upon having local journaling already established. Local journaling on the production side allows each change that ensues for a journal-eligible object e.g., database physical file, SQL table, data area, data queue, byte stream file residing within the IFS) to be recorded and logged. It's these local images that flow to the remote system. Once there, the journal entries serve a variety of purposes, from feeding a high availability software replay program or data warehouse to offering an offline, realtime vault of the most recent database changes.
Reference(s) used for this question:
The Essential Guide to Remote Journaling by IBM
and
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.
and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 286).

QUESTION 54
All of the following can be considered essential business functions that should be identified when creating a Business Impact Analysis (BIA) except one. Which of the following would not be considered an essential element of the BIA but an important TOPIC to include within the BCP plan:

A. IT Network Support
B. Accounting
C. Public Relations
D. Purchasing

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Public Relations, although important to a company, is not listed as an essential business function that should be identified and have loss criteria developed for. All other entries are considered essential and should be identified and have loss criteria developed.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 9: Disaster Recovery and Business continuity (page 598).

QUESTION 55
Of the following, which is NOT a specific loss criteria that should be considered while developing a BIA?

A. Loss of skilled workers knowledge
B. Loss in revenue
C. Loss in profits
D. Loss in reputation

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Although a loss of skilled workers knowledge would cause the company a great loss, it is not identified as a specific loss criteria. It would fall under one of the three other criteria listed as distracters.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 9: Disaster Recovery and Business continuity (page 598).

QUESTION 56
Of the reasons why a Disaster Recovery plan gets outdated, which of the following is not true?

A. Personnel turnover
B. Large plans can take a lot of work to maintain
C. Continous auditing makes a Disaster Recovery plan irrelevant
D. Infrastructure and environment changes

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Although a auditing is a part of corporate security, it in no way supercedes the requirments for a disaster recovery plan. All others can be blamed for a plan going out of date. Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 9: Disaster Recovery and Business continuity (page 609).

QUESTION 57
Which backup type run at regular intervals would take the least time to complete?

A. Full Backup
B. Differential Backup

C. Incremental Backup

D. Disk Mirroring

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Incremental backups only backup changed data (changes archive bit to not backup again if not changed).
Although the incremental backup is fastest to backup, it is usually more time consuming for the restore process.
In some cases, the window available for backup may not be long enough to backup all the data on the system during each backup. In that case, differential or incremental backups may be more appropriate.
In an incremental backup, only the files that changed since the last backup will be backed up. In a differential backup, only the files that changed since the last full backup will be backed up. In general, differentials require more space than incremental backups while incremental backups are faster to perform. On the other hand, restoring data from incremental backups requires more time than differential backups. To restore from incremental backups, the last full backup and all of the incremental backups performed are combined. In contrast, restoring from a differential backup requires only the last full backup and the latest differential.
The following are incorrect answers:
Differential backups backup all data since the last full backup (does not reset archive bit) Full backups backup all selected data, regardless of archive bit, and resets the archive bit.
Disk mirroring is not considered as a backup type.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 20385-20390). Auerbach Publications. Kindle Edition.
and
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter
9: Disaster Recovery and Business continuity (page 618).

QUESTION 58
What is electronic vaulting?

A. Information is backed up to tape on a hourly basis and is stored in a on-site vault.

B. Information is backed up to tape on a daily basis and is stored in a on-site vault.

C. Transferring electronic journals or transaction logs to an off-site storage facility

D. A transfer of bulk information to a remote central backup facility.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Electronic vaulting is defined as "a method of transferring bulk information to off-site facilities for backup purposes". Remote Journaling is the same concept as electronic vaulting, but has to do with journals and transaction logs, not the actual files. Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 9: Disaster Recovery and Business continuity (page 619).

QUESTION 59
After a company is out of an emergency state, what should be moved back to the original site first?

A. Executives

B. Least critical components

C. IT support staff

D. Most critical components

Correct Answer: B

Explanation

Explanation/Reference:
Explanation: This will expose any weaknesses in the plan and ensure the primary site has been properly repaired before moving back. Moving critical assets first may induce a second disaster if the primary site has not been repaired properly.
The first group to go back would test items such as connectivity, HVAC, power, water, improper procedures, and/or steps that has been overlooked or not done properly. By moving these first, and fixing any problems identified, the critical operations of the company are not negatively affected.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 9: Disaster Recovery and Business continuity (page 621).

QUESTION 60
How often should tests and disaster recovery drills be performed?

A. At least once a quarter
B. At least once every 6 months
C. At least once a year
D. At least once every 2 years

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Tests and disaster recovery drills should be performed at least once a year. The company should have no confidence in an untested plan. Since systems and processes can change, frequent testing will aid in ensuring a plan will succeed. Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 9: Disaster Recovery and Business continuity (page 621).

QUESTION 61
Business Continuity Planning (BCP) is not defined as a preparation that facilitates:

A. the rapid recovery of mission-critical business operations
B. the continuation of critical business functions
C. the monitoring of threat activity for adjustment of technical controls
D. the reduction of the impact of a disaster

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Although important, The monitoring of threat activity for adjustment of technical controls is not facilitated by a Business Continuity Planning The following answers are incorrect:
All of the other choices are facilitated by a BCP:
the continuation of critical business functions
the rapid recovery of mission-critical business operations the reduction of the impact of a disaster

QUESTION 62
Which of the following is true about Kerberos?

A. It utilizes public key cryptography.
B. It encrypts data after a ticket is granted, but passwords are exchanged in plain text.
C. It depends upon symmetric ciphers.
D. It is a second party authentication system.

Correct Answer: C

Explanation

Explanation/Reference:
Explanation: Kerberos depends on secret keys (symmetric ciphers). Kerberos is a third party authentication protocol. It was designed and developed in the mid 1980's by MIT. It is considered open source but is copyrighted and owned by MIT. It relies on the user's secret keys. The password is used to encrypt and decrypt the keys.
The following answers are incorrect:
It utilizes public key cryptography. Is incorrect because Kerberos depends on secret keys (symmetric ciphers). It encrypts data after a ticket is granted, but passwords are exchanged in plain text. Is incorrect because the passwords are not exchanged but used for encryption and decryption of the keys. It is a second party authentication system. Is incorrect because Kerberos is a third party authentication system, you authenticate to the third party (Kerberos) and not the system you are accessing.

MIT http://web.mit.edu/kerberos/
Wikipedi http://en.wikipedia.org/wiki/Kerberos_%28protocol%29 OIG CBK Access Control (pages 181 - 184)
AIOv3 Access Control (pages 151 - 155)

QUESTION 63
The RSA algorithm is an example of what type of cryptography?

A. Asymmetric Key.
B. Symmetric Key.
C. Secret Key.
D. Private Key.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The following answers are incorrect.
Symmetric Key. Is incorrect because RSA is a Public Key or a Asymmetric Key cryptographic system and not a Symmetric Key or a Secret Key cryptographic system. Secret Key. Is incorrect because RSA is a Public Key or a Asymmetric Key cryptographic system and not a Secret Key or a Symmetric Key cryptographic system. Private Key. Is incorrect because Private Key is just one part if an Asymmetric Key cryptographic system, a Private Key used alone is also called a Symmetric Key cryptographic system.

QUESTION 64
Kerberos depends upon what encryption method?

A. Public Key cryptography.
B. Secret Key cryptography.
C. El Gamal cryptography.
D. Blowfish cryptography.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Kerberos depends on Secret Keys or Symmetric Key cryptography. Kerberos a third party authentication protocol. It was designed and developed in the mid 1980's by MIT. It is considered open source but is copyrighted and owned by MIT. It relies on the user's secret keys. The password is used to encrypt and decrypt the keys. This question asked specifically about encryption methods. Encryption methods can be SYMMETRIC (or secret key) in which encryption and decryption keys are the same, or ASYMMETRIC (aka 'Public Key') in which encryption and decryption keys differ. 'Public Key' methods must be asymmetric, to the extent that the decryption key CANNOT be easily derived from the encryption key. Symmetric keys, however, usually encrypt more efficiently, so they lend themselves to encrypting large amounts of data. Asymmetric

encryption is often limited to ONLY encrypting a symmetric key and other information that is needed in order to decrypt a data stream, and the remainder of the encrypted data uses the symmetric key method for performance reasons. This does not in any way diminish the security nor the ability to use a public key to encrypt the data, since the symmetric key method is likely to be even MORE secure than the asymmetric method.
For symmetric key ciphers, there are basically two types: BLOCK CIPHERS, in which a fixed length block is encrypted, and STREAM CIPHERS, in which the data is encrypted one 'data unit' (typically 1 byte) at a time, in the same order it was received in.
The following answers are incorrect:
Public Key cryptography. Is incorrect because Kerberos depends on Secret Keys or Symmetric Key cryptography and not Public Key or Asymmetric Key cryptography. El Gamal cryptography. Is incorrect because El Gamal is an Asymmetric Key encryption algorithm. Blowfish cryptography. Is incorrect because Blowfish is a Symmetric Key encryption algorithm.

OIG CBK Access Control (pages 181 - 184)
AIOv3 Access Control (pages 151 - 155)
Wikipedia http://en.wikipedia.org/wiki/Blowfish_%28cipher%29 ; http://en.wikipedia.org/wiki/El_Gamal
http://www.mrp3.com/encrypt.html

QUESTION 65
The DES algorithm is an example of what type of cryptography?

A. Secret Key
B. Two-key
C. Asymmetric Key
D. Public Key

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: DES is also known as a Symmetric Key or Secret Key algorithm. DES is a Symmetric Key algorithm, meaning the same key is used for encryption and decryption.
For the exam remember that:
DES key Sequence is 8 Bytes or 64 bits (8 x 8 = 64 bits) DES has an Effective key length of only 56 Bits. 8 of the Bits are used for parity purpose only.
DES has a total key length of 64 Bits.
The following answers are incorrect:
Two-key This is incorrect because DES uses the same key for encryption and decryption. Asymmetric Key This is incorrect because DES is a Symmetric Key algorithm using the same key for encryption and decryption and an Asymmetric Key algorithm uses both a Public Key and a Private Key.
Public Key. This is incorrect because Public Key or algorithm Asymmetric Key does not use the same key is used for encryption and decryption.
References used for this question:
http://en.wikipedia.org/wiki/Data_Encryption_Standard

QUESTION 66
Which of the following encryption methods is known to be unbreakable?

A. Symmetric ciphers.
B. DES codebooks.
C. One-time pads.
D. Elliptic Curve Cryptography.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: A One-Time Pad uses a keystream string of bits that is generated completely at random that is used only once. Because it is used only once it is considered unbreakable.
The following answers are incorrect:
Symmetric ciphers. This is incorrect because a Symmetric Cipher is created by substitution and transposition. They can and have been broken
DES codebooks. This is incorrect because Data Encryption Standard (DES) has been broken, it was replaced by Advanced Encryption Standard (AES).
Elliptic Curve Cryptography. This is incorrect because Elliptic Curve Cryptography or ECC is typically used on wireless devices such as cellular phones that have small processors. Because of the lack of processing power the keys used at often small. The smaller the key, the easier it is considered to be breakable. Also, the technology has not been around long enough or tested thourough enough to be considered truly unbreakable.

QUESTION 67
What algorithm was DES derived from?

A. Twofish.
B. Skipjack.
C. Brooks-Aldeman.
D. Lucifer.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: NSA took the 128-bit algorithm Lucifer that IBM developed, reduced the key size to 64 bits and with that developed DES.
The following answers are incorrect:
Twofish. This is incorrect because Twofish is related to Blowfish as a possible replacement for DES.
Skipjack. This is incorrect, Skipjack was developed after DES by the NSA . Brooks-Aldeman. This is incorrect because this is a distractor, no algorithm exists with this name.

QUESTION 68
What is a characteristic of using the Electronic Code Book mode of DES encryption?

A. A given block of plaintext and a given key will always produce the same ciphertext.
B. Repetitive encryption obscures any repeated patterns that may have been present in the plaintext.
C. Individual characters are encoded by combining output from earlier encryption routines with plaintext.
D. The previous DES output is used as input.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: A given message and key always produce the same ciphertext.
The following answers are incorrect:
Repetitive encryption obscures any repeated patterns that may have been present in the plaintext. Is incorrect because with Electronic Code Book a given 64 bit block of plaintext always produces the same ciphertext
Individual characters are encoded by combining output from earlier encryption routines with plaintext. This is incorrect because with Electronic Code Book processing 64 bits at a time until the end of the file was reached. This is a characteristic of Cipher Feedback. Cipher Feedback the ciphertext is run through a key-generating device to create the key for the next block of plaintext. The previous DES output is used as input. Is incorrect because This is incorrect because with Electronic Code Book processing 64 bits at a time until the end of the file was reached . This is a characteristic of Cipher Block Chaining. Cipher Block Chaining uses the output from the previous block to encrypt the next block.

QUESTION 69

Where parties do not have a shared secret and large quantities of sensitive information must be passed, the most efficient means of transferring information is to use Hybrid Encryption Methods.
What does this mean?

A. Use of public key encryption to secure a secret key, and message encryption using the secret key.
B. Use of the recipient's public key for encryption and decryption based on the recipient's private key.
C. Use of software encryption assisted by a hardware encryption accelerator.
D. Use of elliptic curve encryption.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: A Public Key is also known as an asymmetric algorithm and the use of a secret key would be a symmetric algorithm.
The following answers are incorrect:
Use of the recipient's public key for encryption and decryption based on the recipient's private key. Is incorrect this would be known as an asymmetric algorithm. Use of software encryption assisted by a hardware encryption accelerator. This is incorrect, it is a distractor.
Use of Elliptic Curve Encryption. Is incorrect this would use an asymmetric algorithm.

QUESTION 70
Public Key Infrastructure (PKI) uses asymmetric key encryption between parties. The originator encrypts information using the intended recipient's "public" key in order to get confidentiality of the data being sent. The recipients use their own "private" key to decrypt the information. The "Infrastructure" of this methodology ensures that:

A. The sender and recipient have reached a mutual agreement on the encryption key exchange that they will use.
B. The channels through which the information flows are secure.
C. The recipient's identity can be positively verified by the sender.
D. The sender of the message is the only other person with access to the recipient's private key.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Through the use of Public Key Infrastructure (PKI) the recipient's identity can be positively verified by the sender.
The sender of the message knows he is using a Public Key that belongs to a specific user. He can validate through the Certification Authority (CA) that a public key is in fact the valid public key of the receiver and the receiver is really who he claims to be. By using the public key of the recipient, only the recipient using the matching private key will be able to decrypt the message. When you wish to achieve confidentiality, you encrypt the message with the recipient public key. If the sender would wish to prove to the recipient that he is really who he claims to be then the sender would apply a digital signature on the message before encrypting it with the public key of the receiver. This would provide Confidentiality and Authenticity of the message. A PKI (Public Key Infrastructure) enables users of an insecure public network, such as the Internet, to securely and privately exchange data through the use of public key-pairs that are obtained and shared through a trusted authority, usually referred to as a Certificate Authority. The PKI provides for digital certificates that can vouch for the identity of individuals or organizations, and for directory services that can store, and when necessary, revoke those digital certificates. A PKI is the underlying technology that addresses the issue of trust in a normally untrusted environment.
The following answers are incorrect:
The sender and recipient have reached a mutual agreement on the encryption key exchange that they will use. Is incorrect because through the use of Public Key Infrastructure (PKI), the parties do not have to have a mutual agreement. They have a trusted 3rd party Certificate Authority to perform the verification of the sender.
The channels through which the information flows are secure. Is incorrect because the use of Public Key

Infrastructure (PKI) does nothing to secure the channels. The sender of the message is the only other person with access to the recipient's private key. Is incorrect because the sender does not have access to the recipient's private key though Public Key Infrastructure (PKI).
Reference(s) used for this question:
OIG CBK Cryptography (pages 253 - 254)

QUESTION 71
Which of the following statements is true about data encryption as a method of protecting data?

A. It should sometimes be used for password files
B. It is usually easily administered
C. It makes few demands on system resources
D. It requires careful key management

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: In cryptography, you always assume the "bad guy" has the encryption algorithm (indeed, many algorithms such as DES, Triple DES, AES, etc. are public domain). What the bad guy lacks is the key used to complete that algorithm and encrypt/decrypt information. Therefore, protection of the key, controlled distribution, scheduled key change, timely destruction, and several other factors require careful consideration. All of these factors are covered under the umbrella term of "key management".
Another significant consideration is the case of "data encryption as a method of protecting data" as the question states. If that data is to be stored over a long period of time (such as on backup), you must ensure that your key management scheme stores old keys for as long as they will be needed to decrypt the information they encrypted.
The other answers are not correct because:
"It should sometimes be used for password files." - Encryption is often used to encrypt passwords stored within password files, but it is not typically effective for the password file itself. On most systems, if a user cannot access the contents of a password file, they cannot authenticate.
Encrypting the entire file prevents that access.
"It is usually easily administered." - Developments over the last several years have made cryptography significantly easier to manage and administer. But it remains a significant challenge.
This is not a good answer.
"It makes few demands on system resources." - Cryptography is, essentially, a large complex mathematical algorithm. In order to encrypt and decrypt information, the system must perform this algorithm hundreds, thousands, or even millions/billions/trillions of times. This becomes system resource intensive, making this a very bad answer.
Official ISC2 Guide page: 266 (poor explanation)
All in One Third Edition page: 657 (excellent explanation) Key Management - Page 732, All in One Fourth Edition

QUESTION 72
Which type of algorithm is considered to have the highest strength per bit of key length of any of the asymmetric algorithms?

A. Rivest, Shamir, Adleman (RSA)
B. El Gamal
C. Elliptic Curve Cryptography (ECC)
D. Advanced Encryption Standard (AES)

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The other answers are not correct because:

"Rivest, Shamir, Adleman (RSA)" is incorrect because RSA is a "traditional" asymmetric algorithm. While it is reasonably strong, it is not considered to be as strong as ECC based systems. "El Gamal" is incorrect because it is also a "traditional" asymmetric algorithm and not considered as strong as ECC based systems.
"Advanced Encryption Standard (AES)" is incorrect because the question asks specifically about asymmetric algorithms and AES is a symmetric algorithm.
Official ISC2 Guide page: 258
All in One Third Edition page: 638
The RSA Crypto FAQ: http://www.rsa.com/rsalabs/node.asp?id=2241

QUESTION 73
How many bits is the effective length of the key of the Data Encryption Standard algorithm?

A. 168

B. 128

C. 56

D. 64

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The correct answer is "56". This is actually a bit of a trick question, since the actual key length is 64 bits. However, every eighth bit is ignored because it is used for parity. This makes the "effective length of the key" that the question actually asks for 56 bits.
The other answers are not correct because:
168 - This is the number of effective bits in Triple DES (56 times 3). 128 - Many encryption algorithms use 128 bit key, but not DES. Note that you may see 128 bit encryption referred to as "military strength encryption" because many military systems use key of this length.
64 - This is the actual length of a DES encryption key, but not the "effective length" of the DES key.
Official ISC2 Guide page: 238
All in One Third Edition page: 622

QUESTION 74
The primary purpose for using one-way hashing of user passwords within a password file is which of the following?

A. It prevents an unauthorized person from trying multiple passwords in one logon attempt.

B. It prevents an unauthorized person from reading the password.

C. It minimizes the amount of storage required for user passwords.

D. It minimizes the amount of processing time used for encrypting passwords.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The whole idea behind a one-way hash is that it should be just that - one-way. In other words, an attacker should not be able to figure out your password from the hashed version of that password in any mathematically feasible way (or within any reasonable length of time).
Password Hashing and Encryption
In most situations , if an attacker sniffs your password from the network wire, she still has some work to do before she actually knows your password value because most systems hash the password with a hashing algorithm, commonly MD4 or MD5, to ensure passwords are not sent in cleartext.
Although some people think the world is run by Microsoft, other types of operating systems are out there, such as Unix and Linux. These systems do not use registries and SAM databases, but contain their user passwords in a file cleverly called "shadow." Now, this shadow file does not contain passwords in cleartext; instead, your password is run through a hashing algorithm, and the resulting value is stored in this file.
Unixtype systems zest things up by using salts in this process. Salts are random values added to the

encryption process to add more complexity and randomness. The more randomness entered into the encryption process, the harder it is for the bad guy to decrypt and uncover your password. The use of a salt means that the same password can be encrypted into several thousand different formats. This makes it much more difficult for an attacker to uncover the right format for your system.

Password Cracking tools

Note that the use of one-way hashes for passwords does not prevent password crackers from guessing passwords. A password cracker runs a plain-text string through the same one-way hash algorithm used by the system to generate a hash, then compares that generated has with the one stored on the system. If they match, the password cracker has guessed your password. This is very much the same process used to authenticate you to a system via a password. When you type your username and password, the system hashes the password you typed and compares that generated hash against the one stored on the system - if they match, you are authenticated. Pre-Computed password tables exists today and they allow you to crack passwords on Lan Manager (LM) within a VERY short period of time through the use of Rainbow Tables. A Rainbow Table is a precomputed table for reversing cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering a plaintext password up to a certain length consisting of a limited set of characters. It is a practical example of a space/time trade-off also called a Time-Memory trade off, using more computer processing time at the cost of less storage when calculating a hash on every attempt, or less processing time and more storage when compared to a simple lookup table with one entry per hash. Use of a key derivation function that employs a salt makes this attack unfeasible.

You may want to review "Rainbow Tables" at the links:

http://en.wikipedia.org/wiki/Rainbow_table

http://www.antsight.com/zsl/rainbowcrack/

Today's password crackers:

Meet oclHashcat. They are GPGPU-based multi-hash cracker using a brute-force attack (implemented as mask attack), combinator attack, dictionary attack, hybrid attack, mask attack, and rule-based attack.

This GPU cracker is a fusioned version of oclHashcat-plus and oclHashcat-lite, both very wellknown suites at that time, but now deprecated. There also existed a now very old oclHashcat GPU cracker that was replaced w/ plus and lite, which - as said - were then merged into oclHashcat 1.00 again.

This cracker can crack Hashes of NTLM Version 2 up to 8 characters in less than a few hours. It is definitively a game changer. It can try hundreds of billions of tries per seconds on a very large cluster of GPU's. It supports up to 128 Video Cards at once. I am stuck using Password what can I do to better protect myself?

You could look at safer alternative such as Bcrypt, PBKDF2, and Scrypt. bcrypt is a key derivation function for passwords designed by Niels Provos and David Mazières, based on the Blowfish cipher, and presented at USENIX in 1999. Besides incorporating a salt to protect against rainbow table attacks, bcrypt is an adaptive function: over time, the iteration count can be increased to make it slower, so it remains resistant to brute-force search attacks even with increasing computation power.

In cryptography, scrypt is a password-based key derivation function created by Colin Percival, originally for the Tarsnap online backup service. The algorithm was specifically designed to make it costly to perform large-scale custom hardware attacks by requiring large amounts of memory. In 2012, the scrypt algorithm was published by the IETF as an Internet Draft, intended to become an informational RFC, which has since expired. A simplified version of scrypt is used as a proof-ofwork scheme by a number of cryptocurrencies, such as Litecoin and Dogecoin. PBKDF2 (Password-Based Key Derivation Function 2) is a key derivation function that is part of RSA Laboratories' Public-Key Cryptography Standards (PKCS) series, specifically PKCS #5 v2.0, also published as Internet Engineering Task Force's RFC 2898. It replaces an earlier standard, PBKDF1, which could only produce derived keys up to 160 bits long. PBKDF2 applies a pseudorandom function, such as a cryptographic hash, cipher, or HMAC to the input password or passphrase along with a salt value and repeats the process many times to produce a derived key, which can then be used as a cryptographic key in subsequent operations. The added computational work makes password cracking much more difficult, and is known as key stretching. When the standard was written in 2000, the recommended minimum number of iterations was 1000, but the parameter is intended to be increased over time as CPU speeds increase. Having a salt added to the password reduces the ability to use precomputed hashes (rainbow tables) for attacks, and means that multiple passwords have to be tested individually, not all at once. The standard recommends a salt length of at least 64 bits.

The other answers are incorrect:

"It prevents an unauthorized person from trying multiple passwords in one logon attempt." is incorrect because the fact that a password has been hashed does not prevent this type of brute force password guessing attempt.

"It minimizes the amount of storage required for user passwords" is incorrect because hash algorithms always generate the same number of bits, regardless of the length of the input. Therefore, even short passwords will

still result in a longer hash and not minimize storage requirements.
"It minimizes the amount of processing time used for encrypting passwords" is incorrect because the processing time to encrypt a password would be basically the same required to produce a oneway has of the same password.
Reference(s) used for this question:
http://en.wikipedia.org/wiki/PBKDF2
http://en.wikipedia.org/wiki/Scrypt
http://en.wikipedia.org/wiki/Bcrypt
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 195) . McGraw-Hill.
Kindle Edition.

QUESTION 75
Which of the following issues is not addressed by digital signatures?

A. nonrepudiation
B. authentication
C. data integrity
D. denial-of-service

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: A digital signature directly addresses both confidentiality and integrity of the CIA triad. It does not directly address availability, which is what denial-of-service attacks.
The other answers are not correct because:
"nonrepudiation" is not correct because a digital signature can provide for nonrepudiation. "authentication" is not correct because a digital signature can be used as an authentication mechanism
"data integrity" is not correct because a digital signature does verify data integrity (as part of nonrepudiation)

Official ISC2 Guide page: 227 & 265
All in One Third Edition page: 648

QUESTION 76
Brute force attacks against encryption keys have increased in potency because of increased computing power. Which of the following is often considered a good protection against the brute force cryptography attack?

A. The use of good key generators.
B. The use of session keys.
C. Nothing can defend you against a brute force crypto key attack.
D. Algorithms that are immune to brute force key attacks.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: If we assume a crytpo-system with a large key (and therefore a large key space) a brute force attack will likely take a good deal of time - anywhere from several hours to several years depending on a number of variables. If you use a session key for each message you encrypt, then the brute force attack provides the attacker with only the key for that one message. So, if you are encrypting 10 messages a day, each with a different session key, but it takes me a month to break each session key then I am fighting a loosing battle.
The other answers are not correct because:
"The use of good key generators" is not correct because a brute force key attack will eventually run through all possible combinations of key. Therefore, any key will eventually be broken in this manner given enough time.
"Nothing can defend you against a brute force crypto key attack" is incorrect, and not the best answer listed. While it is technically true that any key will eventually be broken by a brute force attack, the question remains

"how long will it take?". In other words, if you encrypt something today but I can't read it for 10,000 years, will you still care? If the key is changed every session does it matter if it can be broken after the session has ended? Of the answers listed here, session keys are "often considered a good protection against the brute force cryptography attack" as the question asks.
"Algorithms that are immune to brute force key attacks" is incorrect because there currently are no such algorithms.

Official ISC2 Guide page: 259
All in One Third Edition page: 623

QUESTION 77
The Data Encryption Standard (DES) encryption algorithm has which of the following characteristics?

A. 64 bits of data input results in 56 bits of encrypted output
B. 128 bit key with 8 bits used for parity
C. 64 bit blocks with a 64 bit total key length
D. 56 bits of data input results in 56 bits of encrypted output

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: DES works with 64 bit blocks of text using a 64 bit key (with 8 bits used for parity, so the effective key length is 56 bits).
Some people are getting the Key Size and the Block Size mixed up. The block size is usually a specific length. For example DES uses block size of 64 bits which results in 64 bits of encrypted data for each block. AES uses a block size of 128 bits, the block size on AES can only be 128 as per the published standard FIPS-197.
A DES key consists of 64 binary digits ("0"s or "1"s) of which 56 bits are randomly generated and used directly by the algorithm. The other 8 bits, which are not used by the algorithm, may be used for error detection. The 8 error detecting bits are set to make the parity of each 8-bit byte of the key odd, i.e., there is an odd number of "1"s in each 8-bit byte1. Authorized users of encrypted computer data must have the key that was used to encipher the data in order to decrypt it.
IN CONTRAST WITH AES
The input and output for the AES algorithm each consist of sequences of 128 bits (digits with values of 0 or 1). These sequences will sometimes be referred to as blocks and the number of bits they contain will be referred to as their length. The Cipher Key for the AES algorithm is a sequence of 128, 192 or 256 bits. Other input, output and Cipher Key lengths are not permitted by this standard.
The Advanced Encryption Standard (AES) specifies the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. Rijndael was designed to handle additional block sizes and key lengths, however they are not adopted in the AES standard.
The AES algorithm may be used with the three different key lengths indicated above, and therefore these different "flavors" may be referred to as "AES-128", "AES-192", and "AES-256".
The other answers are not correct because:
"64 bits of data input results in 56 bits of encrypted output" is incorrect because while DES does work with 64 bit block input, it results in 64 bit blocks of encrypted output. "128 bit key with 8 bits used for parity" is incorrect because DES does not ever use a 128 bit key. "56 bits of data input results in 56 bits of encrypted output" is incorrect because DES always works with 64 bit blocks of input/output, not 56 bits.
Reference(s) used for this question:
Official ISC2 Guide to the CISSP CBK, Second Edition, page: 336-343 http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

QUESTION 78
PGP uses which of the following to encrypt data?

A. An asymmetric encryption algorithm
B. A symmetric encryption algorithm
C. A symmetric key distribution system

D. An X.509 digital certificate

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Notice that the question specifically asks what PGP uses to encrypt For this, PGP uses an symmetric key algorithm. PGP then uses an asymmetric key algorithm to encrypt the session key and then send it securely to the receiver. It is an hybrid system where both types of ciphers are being used for different purposes.
Whenever a question talks about the bulk of the data to be sent, Symmetric is always best to choice to use because of the inherent speed within Symmetric Ciphers. Asymmetric ciphers are 100 to 1000 times slower than Symmetric Ciphers.
The other answers are not correct because:
"An asymmetric encryption algorithm" is incorrect because PGP uses a symmetric algorithm to encrypt data.
"A symmetric key distribution system" is incorrect because PGP uses an asymmetric algorithm for the distribution of the session keys used for the bulk of the data. "An X.509 digital certificate" is incorrect because PGP does not use X.509 digital certificates to encrypt the data, it uses a session key to encrypt the data.

Official ISC2 Guide page: 275
All in One Third Edition page: 664 - 665

QUESTION 79
A public key algorithm that does both encryption and digital signature is which of the following?

A. RSA
B. DES
C. IDEA
D. Diffie-Hellman

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: RSA can be used for encryption, key exchange, and digital signatures.
Key Exchange versus key Agreement
KEY EXCHANGE
Key exchange (also known as "key establishment") is any method in cryptography by which cryptographic keys are exchanged between users, allowing use of a cryptographic algorithm. If sender and receiver wish to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt messages received. The nature of the equipping they require depends on the encryption technique they might use. If they use a code, both will require a copy of the same codebook. If they use a cipher, they will need appropriate keys. If the cipher is a symmetric key cipher, both will need a copy of the same key. If an asymmetric key cipher with the public/private key property, both will need the other's public key.
KEY AGREEMENT
Diffie-Hellman is a key agreement algorithm used by two parties to agree on a shared secret. The Diffie Hellman (DH) key agreement algorithm describes a means for two parties to agree upon a shared secret over a public network in such a way that the secret will be unavailable to eavesdroppers. The DH algorithm converts the shared secret into an arbitrary amount of keying material. The resulting keying material is used as a symmetric encryption key.
The other answers are not correct because:
DES and IDEA are both symmetric algorithms.
Diffie-Hellman is a common asymmetric algorithm, but is used only for key agreement. It is not typically used for data encryption and does not have digital signature capability.

http://tools.ietf.org/html/rfc2631
For Diffie-Hellman information: http://www.netip.com/articles/keith/diffie-helman.htm

QUESTION 80
Which of the following identifies the encryption algorithm selected by NIST for the new Advanced Encryption Standard?

A. Twofish
B. Serpent
C. RC6
D. Rijndael

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The
Answer: Rijndael. Rijndael is the new approved method of encrypting sensitive but unclassified information for the U.S. government. It has been accepted by and is also widely used in the public arena as well. It has low memory requirements and has been constructed to easily defend against timing attacks.
The following answers are incorrect: Twofish. Twofish was among the final candidates chosen for AES, but was not selected.
Serpent. Serpent was among the final candidates chosen for AES, but was not selected. RC6. RC6 was among the final candidates chosen for AES, but was not selected. The following reference(s) were/was used to create this question:
ISC2 OIG, 2007 p. 622, 629-630
Shon Harris AIO, v.3 p 247-250

QUESTION 81
Compared to RSA, which of the following is true of Elliptic Curve Cryptography(ECC)?

A. It has been mathematically proved to be more secure.
B. It has been mathematically proved to be less secure.
C. It is believed to require longer key for equivalent security.
D. It is believed to require shorter keys for equivalent security.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The following answers are incorrect: It has been mathematically proved to be less secure. ECC has not been proved to be more or less secure than RS A. Since ECC is newer than
RSA, it is considered riskier by some, but that is just a general assessment, not based on mathematical arguments.
It has been mathematically proved to be more secure. ECC has not been proved to be more or less secure than RS
A. Since ECC is newer than RSA, it is considered riskier by some, but that is just a general assessment, not based on mathematical arguments. It is believed to require longer key for equivalent security. On the contrary, it is believed to require shorter keys for equivalent security of RSA.
Shon Harris, AIO v5 pg719 states:
"In most cases, the longer the key, the more protection that is provided, but ECC can provide the same level of protection with a key size that is shorter that what RSA requires" The following reference(s) were/was used to create this question:
ISC2 OIG, 2007 p. 258
Shon Harris, AIO v5 pg719

QUESTION 82
What are the three most important functions that Digital Signatures perform?

A. Integrity, Confidentiality and Authorization

B. Integrity, Authentication and Nonrepudiation
C. Authorization, Authentication and Nonrepudiation
D. Authorization, Detection and Accountability

Correct Answer: B
Explanation

Explanation/Reference:
TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2.

QUESTION 83
Which of the following protocols that provide integrity and authentication for IPSec, can also provide non-repudiation in IPSec?

A. Authentication Header (AH)
B. Encapsulating Security Payload (ESP)
C. Secure Sockets Layer (SSL)
D. Secure Shell (SSH-2)

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: As per the RFC in reference, the Authentication Header (AH) protocol is a mechanism for providing strong integrity and authentication for IP datagrams. It might also provide non-repudiation, depending on which cryptographic algorithm is used and how keying is performed. For example, use of an asymmetric digital signature algorithm, such as RSA, could provide non-repudiation.
from a cryptography point of view, so we will cover it from a VPN point of view here. IPSec is a suite of protocols that was developed to specifically protect IP traffic. IPv4 does not have any integrated security, so IPSec was developed to bolt onto IP and secure the data the protocol transmits. Where PPTP and L2TP work at the data link layer, IPSec works at the network layer of the OSI model. The main protocols that make up the IPSec suite and their basic functionality are as follows:
A. Authentication Header (AH) provides data integrity, data origin authentication, and protection from replay attacks. B. Encapsulating Security Payload (ESP) provides confidentiality, data-origin authentication, and data integrity. C. Internet Security Association and Key Management Protocol (ISAKMP) provides a framework for security association creation and key exchange. D. Internet Key Exchange (IKE) provides authenticated keying material for use with ISAKMP.
The following are incorrect answers:
ESP is a mechanism for providing integrity and confidentiality to IP datagrams. It may also provide authentication, depending on which lgorithm and algorithm mode are used. Non-repudiation and protection from traffic analysis are not provided by ESP (RFC 1827). SSL is a secure protocol used for transmitting private information over the Internet. It works by using a public key to encrypt data that is transferred of the SSL connection. OIG 2007, page 976 SSH-2 is a secure, efficient, and portable version of SSH (Secure Shell) which is a secure replacement for telnet.
Reference(s) used for this question:
Shon Harris, CISSP All In One, 6th Edition , Page 705
and
RFC 1826, http://tools.ietf.org/html/rfc1826, paragraph 1.

QUESTION 84
Which of the following is a cryptographic protocol and infrastructure developed to send encrypted credit card numbers over the Internet?

A. Secure Electronic Transaction (SET)
B. MONDEX
C. Secure Shell (SSH-2)

D. Secure Hypertext Transfer Protocol (S-HTTP)

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: SET was developed by a consortium including Visa and MasterCard. Source: Harris, Shon, CISSP All In One Exam Guide, pages 668-669. Mondex is a smart card electronic cash system owned by MasterCard. SSH-2 is a secure, efficient, and portable version of SSH (Secure Shell) which is a secure replacement for telnet.
Secure HTTP is a secure message-oriented communications protocol designed for use in conjunction with HTTP. It is designed to coexist with HTTP's messaging model and to be easily integrated with HTTP applications.

QUESTION 85
Which of the following cryptographic attacks describes when the attacker has a copy of the plaintext and the corresponding ciphertext?

A. known plaintext
B. brute force
C. ciphertext only
D. chosen plaintext

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The goal to this type of attack is to find the cryptographic key that was used to encrypt the message. Once the key has been found, the attacker would then be able to decrypt all messages that had been encrypted using that key.
The known-plaintext attack (KPA) or crib is an attack model for cryptanalysis where the attacker has samples of both the plaintext and its encrypted version (ciphertext), and is at liberty to make use of them to reveal further secret information such as secret keys and code books. The term "crib" originated at Bletchley Park, the British World War II decryption operation In cryptography, a brute force attack or exhaustive key search is a strategy that can in theory be used against any encrypted data by an attacker who is unable to take advantage of any weakness in an encryption system that would otherwise make his task easier. It involves systematically checking all possible keys until the correct key is found. In the worst case, this would involve traversing the entire key space, also called search space. In cryptography, a ciphertext-only attack (COA) or known ciphertext attack is an attack model for cryptanalysis where the attacker is assumed to have access only to a set of ciphertexts. The attack is completely successful if the corresponding plaintexts can be deduced, or even better, the key. The ability to obtain any information at all about the underlying plaintext is still considered a success. For example, if an adversary is sending ciphertext continuously to maintain traffic-flow security, it would be very useful to be able to distinguish real messages from nulls. Even making an informed guess of the existence of real messages would facilitate traffic analysis. In the history of cryptography, early ciphers, implemented using pen-and-paper, were routinely broken using ciphertexts alone. Cryptographers developed statistical techniques for attacking ciphertext, such as frequency analysis. Mechanical encryption devices such as Enigma made these attacks much more difficult (although, historically, Polish cryptographers were able to mount a successful ciphertext-only cryptanalysis of the Enigma by exploiting an insecure protocol for indicating the message settings).
Every modern cipher attempts to provide protection against ciphertext-only attacks. The vetting process for a new cipher design standard usually takes many years and includes exhaustive testing of large quantities of ciphertext for any statistical departure from random noise. See:
Advanced Encryption Standard process. Also, the field of steganography evolved, in part, to develop methods like mimic functions that allow one piece of data to adopt the statistical profile of another. Nonetheless poor cipher usage or reliance on home-grown proprietary algorithms that have not been subject to thorough scrutiny has resulted in many computer-age encryption systems that are still subject to ciphertext-only attack.
Examples include:
Early versions of Microsoft's PPTP virtual private network software used the same RC4 key for the sender and

the receiver (later versions had other problems). In any case where a stream cipher like RC4 is used twice with the same key it is open to ciphertext-only attack. See: stream cipher attack
Wired Equivalent Privacy (WEP), the first security protocol for Wi-Fi, proved vulnerable to several attacks, most of them ciphertext-only.
A chosen-plaintext attack (CPA) is an attack model for cryptanalysis which presumes that the attacker has the capability to choose arbitrary plaintexts to be encrypted and obtain the corresponding ciphertexts. The goal of the attack is to gain some further information which reduces the security of the encryption scheme. In the worst case, a chosen-plaintext attack could reveal the scheme's secret key.
This appears, at first glance, to be an unrealistic model; it would certainly be unlikely that an attacker could persuade a human cryptographer to encrypt large amounts of plaintexts of the attacker's choosing. Modern cryptography, on the other hand, is implemented in software or hardware and is used for a diverse range of applications; for many cases, a chosen-plaintext attack is often very feasible. Chosen-plaintext attacks become extremely important in the context of public key cryptography, where the encryption key is public and attackers can encrypt any plaintext they choose.
Any cipher that can prevent chosen-plaintext attacks is then also guaranteed to be secure against known-plaintext and ciphertext-only attacks; this is a conservative approach to security. Two forms of chosen-plaintext attack can be distinguished:
Batch chosen-plaintext attack, where the cryptanalyst chooses all plaintexts before any of them are encrypted. This is often the meaning of an unqualified use of "chosen-plaintext attack". Adaptive chosen-plaintext attack, where the cryptanalyst makes a series of interactive queries, choosing subsequent plaintexts based on the information from the previous encryptions.

Source: TIPTON, Harold, Official (ISC)2 Guide to the CISSP CBK (2007), page 271.
and
Wikipedia at the following links:
http://en.wikipedia.org/wiki/Chosen-plaintext_attack
http://en.wikipedia.org/wiki/Known-plaintext_attack
http://en.wikipedia.org/wiki/Ciphertext-only_attack
http://en.wikipedia.org/wiki/Brute_force_attack

QUESTION 86
Which of the following is NOT a true statement regarding the implementaton of the 3DES modes?

A. DES-EEE1 uses one key
B. DES-EEE2 uses two keys
C. DES-EEE3 uses three keys
D. DES-EDE2 uses two keys

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: There is no DES mode call DES-EEE1. It does not exist. The following are the correct modes for triple-DES (3DES):
DES-EEE3 uses three keys for encryption and the data is encrypted, encrypted, encrypted; DES-EDE3 uses three keys and encrypts, decrypts and encrypts data. DES-EEE2 and DES-EDE2 are the same as the previous modes, but the first and third operations use the same key.
Reference(s) used for this question:
Shon Harris, CISSP All In One (AIO) book, 6th edition , page 808 and
Official ISC2 Guide to the CISSP CBK, 2nd Edition (2010) , page 344-345

QUESTION 87
Which of the following ciphers is a subset on which the Vigenere polyalphabetic cipher was based on?

A. Caesar
B. The Jefferson disks
C. Enigma

D. SIGABA

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: In cryptography, a Caesar cipher, also known as Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a left shift of 3, D would be replaced by A, E would become B, and so on. The method is named after Julius Caesar, who used it in his private correspondence.
The encryption step performed by a Caesar cipher is often incorporated as part of more complex schemes, such as the Vigenère cipher, and still has modern application in the ROT13 system. As with all single alphabet substitution ciphers, the Caesar cipher is easily broken and in modern practice offers essentially no communication security.
The following answer were incorrect:
The Jefferson disk, or wheel cipher as Thomas Jefferson named it, also known as the Bazeries Cylinder, is a cipher system using a set of wheels or disks, each with the 26 letters of the alphabet arranged around their edge. The order of the letters is different for each disk and is usually scrambled in some random way. Each disk is marked with a unique number. A hole in the centre of the disks allows them to be stacked on an axle. The disks are removable and can be mounted on the axle in any order desired. The order of the disks is the cipher key, and both sender and receiver must arrange the disks in the same predefined order. Jefferson's device had 36 disks. An Enigma machine is any of a family of related electro-mechanical rotor cipher machines used for the encryption and decryption of secret messages. Enigma was invented by the German engineer Arthur Scherbius at the end of World War I. The early models were used commercially from the early 1920s, and adopted by military and government services of several countries. Several different Enigma models were produced, but the German military models are the ones most commonly discussed.
SIGABA: In the history of cryptography, the ECM Mark II was a cipher machine used by the United States for message encryption from World War II until the 1950s. The machine was also known as the SIGABA or Converter M-134 by the Army, or CSP-888/889 by the Navy, and a modified Navy version was termed the CSP-2900. Like many machines of the era it used an electromechanical system of rotors in order to encipher messages, but with a number of security improvements over previous designs. No successful cryptanalysis of the machine during its service lifetime is publicly known.
Reference(s) used for this question:
http://en.wikipedia.org/wiki/Jefferson_disk
http://en.wikipedia.org/wiki/Sigaba
http://en.wikipedia.org/wiki/Enigma_machine

QUESTION 88
In a known plaintext attack, the cryptanalyst has knowledge of which of the following?

A. the ciphertext and the key
B. the plaintext and the secret key
C. both the plaintext and the associated ciphertext of several messages
D. the plaintext and the algorithm

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: In a known plaintext attack, the attacker has the plaintext and ciphertext of one or more messages. The goal is to discover the key used to encrypt the messages so that other messages can be deciphered and read.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 3rd Ed., chapter 8: Cryptography (page 676). Also check out: Handbook of Applied Cryptography 4th Edition by Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone.

QUESTION 89

What is the length of an MD5 message digest?

A. 128 bits
B. 160 bits
C. 256 bits
D. varies depending upon the message size.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: A hash algorithm (alternatively, hash "function") takes binary data, called the message, and produces a condensed representation, called the message digest. A cryptographic hash algorithm is a hash algorithm that is designed to achieve certain security properties. The Federal Information Processing Standard 180-3, Secure Hash Standard, specifies five cryptographic hash algorithms - SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 for federal use in the US; the standard was also widely adopted by the information technology industry and commercial companies.
The MD5 Message-Digest Algorithm is a widely used cryptographic hash function that produces a 128-bit (16-byte) hash value. Specified in RFC 1321, MD5 has been employed in a wide variety of security applications, and is also commonly used to check data integrity. MD5 was designed by Ron Rivest in 1991 to replace an earlier hash function, MD4. An MD5 hash is typically expressed as a 32-digit hexadecimal number.
However, it has since been shown that MD5 is not collision resistant; as such, MD5 is not suitable for applications like SSL certificates or digital signatures that rely on this property. In 1996, a flaw was found with the design of MD5, and while it was not a clearly fatal weakness, cryptographers began recommending the use of other algorithms, such as SHA-1 - which has since been found also to be vulnerable. In 2004, more serious flaws were discovered in MD5, making further use of the algorithm for security purposes questionable - specifically, a group of researchers described how to create a pair of files that share the same MD5 checksum. Further advances were made in breaking MD5 in 2005, 2006, and 2007. In December 2008, a group of researchers used this technique to fake SSL certificate validity, and US-CERT now says that MD5 "should be considered cryptographically broken and unsuitable for further use." and most U.S. government applications now require the SHA-2 family of hash functions.
NIST CRYPTOGRAPHIC HASH PROJECT
NIST announced a public competition in a Federal Register Notice on November 2, 2007 to develop a new cryptographic hash algorithm, called SHA-3, for standardization. The competition was NIST's response to advances made in the cryptanalysis of hash algorithms. NIST received sixty-four entries from cryptographers around the world by October 31, 2008, and selected fifty-one first-round candidates in December 2008, fourteen second-round candidates in July 2009, and five finalists BLAKE, Grøstl, JH, Keccak and Skein, in December 2010 to advance to the third and final round of the competition. Throughout the competition, the cryptographic community has provided an enormous amount of feedback. Most of the comments were sent to NIST and a public hash forum; in addition, many of the cryptanalysis and performance studies were published as papers in major cryptographic conferences or leading cryptographic journals. NIST also hosted a SHA-3 candidate conference in each round to obtain public feedback. Based on the public comments and internal review of the candidates, NIST announced Keccak as the winner of the SHA-3 Cryptographic Hash Algorithm Competition on October 2, 2012, and ended the five-year competition. Tipton, Harold, et. al., Officical (ISC)2 Guide to the CISSP CBK, 2007 edition, page 261.
and
https://secure.wikimedia.org/wikipedia/en/wiki/Md5
and
http://csrc.nist.gov/groups/ST/hash/sha-3/index.html

QUESTION 90
The Secure Hash Algorithm (SHA-1) creates:

A. a fixed length message digest from a fixed length input message
B. a variable length message digest from a variable length input message
C. a fixed length message digest from a variable length input message
D. a variable length message digest from a fixed length input message

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: According to The CISSP Prep Guide, "The Secure Hash Algorithm (SHA-1) computes a fixed length message digest from a variable length input message." Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, page 160.
also see:
http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf

QUESTION 91
The RSA Algorithm uses which mathematical concept as the basis of its encryption?

A. Geometry
B. 16-round ciphers
C. PI (3.14159...)
D. Two large prime numbers

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Source: TIPTON, et. al, Official (ISC)2 Guide to the CISSP CBK, 2007 edition, page 254.
And from the RSA web site, http://www.rsa.com/rsalabs/node.asp?id=2214 :
The RSA cryptosystem is a public-key cryptosystem that offers both encryption and digital signatures (authentication). Ronald Rivest, Adi Shamir, and Leonard Adleman developed the RSA system in 1977 [RSA78]; RSA stands for the first letter in each of its inventors' last names. The RSA algorithm works as follows: take two large primes, p and q, and compute their product n = pq; n is called the modulus. Choose a number, e, less than n and relatively prime to (p-1)(q-1), which means e and (p-1)(q-1) have no common factors except 1. Find another number d such that (ed - 1) is divisible by (p-1)(q-1). The values e and d are called the public and private exponents, respectively. The public key is the pair (n, e); the private key is (n, d). The factors p and q may be destroyed or kept with the private key.
It is currently difficult to obtain the private key d from the public key (n, e). However if one could factor n into p and q, then one could obtain the private key d. Thus the security of the RSA system is based on the assumption that factoring is difficult. The discovery of an easy method of factoring would "break" RSA (see .1.3 and .3.3).
Here is how the RSA system can be used for encryption and digital signatures (in practice, the actual use is slightly different; see questions 3.1.7 and 3.1.8):
Encryption
Suppose Alice wants to send a message m to Bob. Alice creates the ciphertext c by exponentiating: c = me mod n, where e and n are Bob's public key. She sends c to Bob. To decrypt, Bob also exponentiates: m = cd mod n; the relationship between e and d ensures that Bob correctly recovers m. Since only Bob knows d, only Bob can decrypt this message.
Digital Signature
Suppose Alice wants to send a message m to Bob in such a way that Bob is assured the message is both authentic, has not been tampered with, and from Alice. Alice creates a digital signature s by exponentiating: s = md mod n, where d and n are Alice's private key. She sends m and s to Bob. To verify the signature, Bob exponentiates and checks that the message m is recovered: m = se mod n, where e and n are Alice's public key.
Thus encryption and authentication take place without any sharing of private keys: each person uses only another's public key or their own private key. Anyone can send an encrypted message or verify a signed message, but only someone in possession of the correct private key can decrypt or sign a message.

QUESTION 92
The Clipper Chip utilizes which concept in public key cryptography?

A. Substitution
B. Key Escrow
C. An undefined algorithm
D. Super strong encryption

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The Clipper chip is a chipset that was developed and promoted by the U.S. Government as an encryption device to be adopted by telecommunications companies for voice transmission. It was announced in 1993 and by 1996 was entirely defunct. The heart of the concept was key escrow. In the factory, any new telephone or other device with a Clipper chip would be given a "cryptographic key", that would then be provided to the government in "escrow". If government agencies "established their authority" to listen to a communication, then the password would be given to those government agencies, who could then decrypt all data transmitted by that particular telephone.
The CISSP Prep Guide states, "The idea is to divide the key into two parts, and to escrow two portions of the key with two separate 'trusted' organizations. Then, law enforcement officals, after obtaining a court order, can retreive the two pieces of the key from the organizations and decrypt the message."

http://en.wikipedia.org/wiki/Clipper_Chip
and
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, page 166.

QUESTION 93
Which of the following are suitable protocols for securing VPN connections at the lower layers of the OSI model?

A. S/MIME and SSH
B. TLS and SSL
C. IPsec and L2TP
D. PKCS#10 and X.509

Correct Answer: C
Explanation

Explanation/Reference:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw- Hill/Osborne, page 467; SMITH, Richard E., Internet Cryptography, 1997, Addison-Wesley Pub Co.

QUESTION 94
What is the role of IKE within the IPsec protocol?

A. peer authentication and key exchange
B. data encryption
C. data signature
D. enforcing quality of service

Correct Answer: A
Explanation

Explanation/Reference:
RFC 2409: The Internet Key Exchange (IKE); DORASWAMY, Naganand & HARKINS, Dan, Ipsec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks, 1999, Prentice Hall PTR; SMITH, Richard E., Internet Cryptography, 1997, Addison-Wesley Pub Co.

QUESTION 95
In which phase of Internet Key Exchange (IKE) protocol is peer authentication performed?

A. Pre Initialization Phase
B. Phase 1
C. Phase 2
D. No peer authentication is performed

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The Internet Key Exchange (IKE) protocol is a key management protocol standard that is used in conjunction with the IPSec standard. IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard. IPSec can however, be configured without IKE by manually configuring the gateways communicating with each other for example.
A security association (SA) is a relationship between two or more entities that describes how the entities will use security services to communicate securely. In phase 1 of this process, IKE creates an authenticated, secure channel between the two IKE peers, called the IKE security association. The Diffie-Hellman key agreement is always performed in this phase.
In phase 2 IKE negotiates the IPSec security associations and generates the required key material for IPSec. The sender offers one or more transform sets that are used to specify an allowed combination of transforms with their respective settings.
Benefits provided by IKE include:
Eliminates the need to manually specify all the IPSec security parameters in the crypto maps at both peers.
Allows you to specify a lifetime for the IPSec security association. Allows encryption keys to change during IPSec sessions.
Allows IPSec to provide anti-replay services.
Permits Certification Authority (CA) support for a manageable, scalable IPSec implementation.
Allows dynamic authentication of peers.

RFC 2409: The Internet Key Exchange (IKE);
DORASWAMY, Naganand & HARKINS, Dan, Ipsec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks, 1999, Prentice Hall PTR; SMITH, Richard E., Internet Cryptography, 1997, Addison-Wesley Pub Co. http://www.ciscopress.com/articles/article.asp?p=25474

QUESTION 96
What is NOT an authentication method within IKE and IPsec?

A. CHAP
B. Pre shared key
C. certificate based authentication
D. Public key authentication

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: CHAP is not used within IPSEC or IKE. CHAP is an authentication scheme used by Point to Point Protocol (PPP) servers to validate the identity of remote clients. CHAP periodically verifies the identity of the client by using a three-way handshake. This happens at the time of establishing the initial link (LCP), and may happen again at any time afterwards. The verification is based on a shared secret (such as the client user's password). After the completion of the link establishment phase, the authenticator sends a "challenge" message to the peer.
The peer responds with a value calculated using a one-way hash function on the challenge and the secret combined.

The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authenticator acknowledges the authentication; otherwise it should terminate the connection.
At random intervals the authenticator sends a new challenge to the peer and repeats steps 1 through 3.
The following were incorrect answers:
Pre Shared Keys
In cryptography, a pre-shared key or PSK is a shared secret which was previously shared between the two parties using some secure channel before it needs to be used. To build a key from shared secret, the key derivation function should be used. Such systems almost always use symmetric key cryptographic algorithms. The term PSK is used in WiFi encryption such as WEP or WPA, where both the wireless access points (AP) and all clients share the same key. The characteristics of this secret or key are determined by the system which uses it; some system designs require that such keys be in a particular format. It can be a password like 'bret13i', a passphrase like 'Idaho hung gear id gene', or a hexadecimal string like '65E4 E556 8622 EEE1'. The secret is used by all systems involved in the cryptographic processes used to secure the traffic between the systems.
Certificat Based Authentication
The most common form of trusted authentication between parties in the wide world of Web commerce is the exchange of certificates. A certificate is a digital document that at a minimum includes a Distinguished Name (DN) and an associated public key. The certificate is digitally signed by a trusted third party known as the Certificate Authority (CA). The CA vouches for the authenticity of the certificate holder. Each principal in the transaction presents certificate as its credentials. The recipient then validates the certificate's signature against its cache of known and trusted CA certificates. A "personal certificate" identifies an end user in a transaction; a "server certificate" identifies the service provider.
Generally, certificate formats follow the X.509 Version 3 standard. X.509 is part of the Open Systems Interconnect
(OSI) X.500 specification.
Public Key Authentication
Public key authentication is an alternative means of identifying yourself to a login server, instead of typing a password. It is more secure and more flexible, but more difficult to set up. In conventional password authentication, you prove you are who you claim to be by proving that you know the correct password. The only way to prove you know the password is to tell the server what you think the password is. This means that if the server has been hacked, or spoofed an attacker can learn your password.
Public key authentication solves this problem. You generate a key pair, consisting of a public key (which everybody is allowed to know) and a private key (which you keep secret and do not give to anybody). The private key is able to generate signatures. A signature created using your private key cannot be forged by anybody who does not have a copy of that private key; but anybody who has your public key can verify that a particular signature is genuine. So you generate a key pair on your own computer, and you copy the public key to the server. Then, when the server asks you to prove who you are, you can generate a signature using your private key. The server can verify that signature (since it has your public key) and allow you to log in. Now if the server is hacked or spoofed, the attacker does not gain your private key or password; they only gain one signature. And signatures cannot be re-used, so they have gained nothing.
There is a problem with this: if your private key is stored unprotected on your own computer, then anybody who gains access to your computer will be able to generate signatures as if they were you. So they will be able to log in to your server under your account. For this reason, your private key is usually encrypted when it is stored on your local machine, using a passphrase of your choice. In order to generate a signature, you must decrypt the key, so you have to type your passphrase.

RFC 2409: The Internet Key Exchange (IKE); DORASWAMY, Naganand & HARKINS, Dan Ipsec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks, 1999, Prentice Hall PTR; SMITH, Richard E.
Internet Cryptography, 1997, Addison-Wesley Pub Co.; HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw-Hill/Osborne, page 467.
http://en.wikipedia.org/wiki/Pre-shared_key
http://www.home.umk.pl/~mgw/LDAP/RS.C4.JUN.97.pdf
http://the.earth.li/~sgtatham/putty/0.55/htmldoc/Chapter8.html#S8.1

QUESTION 97
What is NOT true with pre shared key authentication within IKE / IPsec protocol?

A. Pre shared key authentication is normally based on simple passwords

B. Needs a Public Key Infrastructure (PKI) to work

C. IKE is used to setup Security Associations

D. IKE builds upon the Oakley protocol and the ISAKMP protocol.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Internet Key Exchange (IKE or IKEv2) is the protocol used to set up a security association (SA) in the IPsec protocol suite. IKE builds upon the Oakley protocol and ISAKMP. IKE uses X.509 certificates for authentication which are either pre-shared or distributed using DNS (preferably with DNSSEC) and a Diffie-Hellman key exchange to set up a shared session secret from which cryptographic keys are derived.
Internet Key Exchange (IKE) Internet key exchange allows communicating partners to prove their identity to each other and establish a secure communication channel, and is applied as an authentication component of IPSec.
IKE uses two phases:
Phase 1: In this phase, the partners authenticate with each other, using one of the following:
Shared Secret: A key that is exchanged by humans via telephone, fax, encrypted e-mail, etc. Public Key Encryption: Digital certificates are exchanged. Revised mode of Public Key Encryption: To reduce the overhead of public key encryption, a nonce (a Cryptographic function that refers to a number or bit string used only once, in security engineering) is encrypted with the communicating partner's public key, and the peer's identity is encrypted with symmetric encryption using the nonce as the key. Next, IKE establishes a temporary security association and secure tunnel to protect the rest of the key exchange. Phase 2:
The peers' security associations are established, using the secure tunnel and temporary SA created at the end of phase 1.
The following reference(s) were used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 7032-7048). Auerbach Publications. Kindle Edition.
and
RFC 2409 at http://tools.ietf.org/html/rfc2409
and
http://en.wikipedia.org/wiki/Internet_Key_Exchange

QUESTION 98
In a hierarchical PKI the highest CA is regularly called Root CA, it is also referred to by which one of the following term?

A. Subordinate CA

B. Top Level CA

C. Big CA

D. Master CA

Correct Answer: B
Explanation

Explanation/Reference:
Arsenault, Turner, Internet X.509 Public Key Infrastructure: Roadmap, Chapter "Terminology".
Also note that sometimes other terms such as Certification Authority Anchor (CAA) might be used within some government organization, Top level CA is another common term to indicate the top level CA, Top Level Anchor could also be used.

QUESTION 99
What is the primary role of cross certification?

A. Creating trust between different PKIs

B. Build an overall PKI hierarchy

C. set up direct trust to a second root CA

D. Prevent the nullification of user certificates by CA certificate revocation

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: More and more organizations are setting up their own internal PKIs. When these independent PKIs need to interconnect to allow for secure communication to take place (either between departments or different companies), there must be a way for the two root CAs to trust each other.
These two CAs do not have a CA above them they can both trust, so they must carry out cross certification. A cross certification is the process undertaken by CAs to establish a trust relationship in which they rely upon each other's digital certificates and public keys as if they had issued them themselves.
When this is set up, a CA for one company can validate digital certificates from the other company and vice versa.
Reference(s) used for this question:
For more information and illustration on Cross certification:
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03qsw p.mspx
http://www.entrust.com/resources/pdf/cross_certification.pdf also see:
Shon Harris, CISSP All in one book, 4th Edition, Page 727 and
RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile; FORD, Warwick & BAUM, Michael S., Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption (2nd Edition), 2000, Prentice Hall PTR, Page 254.

QUESTION 100
What kind of encryption is realized in the S/MIME-standard?

A. Asymmetric encryption scheme

B. Password based encryption scheme

C. Public key based, hybrid encryption scheme

D. Elliptic curve based encryption

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: S/MIME (for Secure MIME, or Secure Multipurpose Mail Extension) is a security process used for e-mail exchanges that makes it possible to guarantee the confidentiality and nonrepudiation of electronic messages.
S/MIME is based on the MIME standard, the goal of which is to let users attach files other than ASCII text files to electronic messages. The MIME standard therefore makes it possible to attach all types of files to e-mails.
S/MIME was originally developed by the company RSA Data Security. Ratified in July 1999 by the IETF, S/MIME has become a standard, whose specifications are contained in RFCs 2630 to 2633.
How S/MIME works
The S/MIME standard is based on the principle of public-key encryption. S/MIME therefore makes it possible to encrypt the content of messages but does not encrypt the communication. The various sections of an electronic message, encoded according to the MIME standard, are each encrypted using a session key.
The session key is inserted in each section's header, and is encrypted using the recipient's public key. Only the recipient can open the message's body, using his private key, which guarantees the confidentiality and integrity of the received message. In addition, the message's signature is encrypted with the sender's private key. Anyone intercepting the communication can read the content of the message's signature, but this ensures the recipient of the sender's identity, since only the sender is capable of encrypting a message (with his private key) that can be decrypted with his public key.
Reference(s) used for this question:
http://en.kioskea.net/contents/139-cryptography-s-mime RFC 2630: Cryptographic Message Syntax;
OPPLIGER, Rolf, Secure Messaging with PGP and S/MIME, 2000, Artech House; HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw-Hill/Osborne, page 570;
SMITH, Richard E., Internet Cryptography, 1997, Addison-Wesley Pub Co.

QUESTION 101
What is the main problem of the renewal of a root CA certificate?

A. It requires key recovery of all end user keys
B. It requires the authentic distribution of the new root CA certificate to all PKI participants
C. It requires the collection of the old root CA certificates from all the users
D. It requires issuance of the new root CA certificate

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The main task here is the authentic distribution of the new root CA certificate as new trust anchor to all the PKI participants (e.g. the users). In some of the rollover-scenarios there is no automatic way, often explicit assignment of trust from each user is needed, which could be very costly.
Other methods make use of the old root CA certificate for automatic trust establishment (see PKIX-reference), but these solutions works only well for scenarios with currently valid root CA certificates (and not for emergency cases e.g. compromise of the current root CA certificate). The rollover of the root CA certificate is a specific and delicate problem and therefore are often ignored during PKI deployment.
Camphausen, I.; Petersen, H.; Stark, C.: Konzepte zum Root CA Zertifikatswechsel, conference Enterprise Security 2002, March 26-27, 2002, Paderborn; RFC 2459 : Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

QUESTION 102
Virus scanning and content inspection of SMIME encrypted e-mail without doing any further processing is:

A. Not possible
B. Only possible with key recovery scheme of all user keys
C. It is possible only if X509 Version 3 certificates are used
D. It is possible only by "brute force" decryption

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Content security measures presumes that the content is available in cleartext on the central mail server.
Encrypted emails have to be decrypted before it can be filtered (e.g. to detect viruses), so you need the decryption key on the central "crypto mail server". There are several ways for such key management, e.g. by message or key recovery methods. However, that would certainly require further processing in order to achieve such goal.

QUESTION 103
What attribute is included in a X.509-certificate?

A. Distinguished name of the subject
B. Telephone number of the department
C. secret key of the issuing CA
D. the key pair of the certificate holder

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: RFC 2459 : Internet X.509 Public Key Infrastructure Certificate and CRL Profile; GUTMANN, P.,

X.509 style guide; SMITH, Richard E., Internet Cryptography, 1997, Addison- Wesley Pub Co.

QUESTION 104
What is the primary role of smartcards in a PKI?

A. Transparent renewal of user keys
B. Easy distribution of the certificates between the users
C. Fast hardware encryption of the raw data
D. Tamper resistant, mobile storage and application of private keys of the users

Correct Answer: D
Explanation

Explanation/Reference:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw- Hill/Osborne, page 139;
SNYDER, J., What is a SMART CARD?.
Wikipedia has a nice definition at: http://en.wikipedia.org/wiki/Tamper_resistance Security
Tamper-resistant microprocessors are used to store and process private or sensitive information, such as private keys or electronic money credit. To prevent an attacker from retrieving or modifying the information, the chips are designed so that the information is not accessible through external means and can be accessed only by the embedded software, which should contain the appropriate security measures.
Examples of tamper-resistant chips include all secure cryptoprocessors, such as the IBM 4758 and chips used in smartcards, as well as the Clipper chip. It has been argued that it is very difficult to make simple electronic devices secure against tampering, because numerous attacks are possible, including:
physical attack of various forms (microprobing, drills, files, solvents, etc.) freezing the device
applying out-of-spec voltages or power surges
applying unusual clock signals
inducing software errors using radiation
measuring the precise time and power requirements of certain operations (see power analysis) Tamper-resistant chips may be designed to zeroise their sensitive data (especially cryptographic keys) if they detect penetration of their security encapsulation or out-of-specification environmental parameters. A chip may even be rated for "cold zeroisation", the ability to zeroise itself even after its power supply has been crippled.
Nevertheless, the fact that an attacker may have the device in his possession for as long as he likes, and perhaps obtain numerous other samples for testing and practice, means that it is practically impossible to totally eliminate tampering by a sufficiently motivated opponent. Because of this, one of the most important elements in protecting a system is overall system design. In particular, tamper-resistant systems should "fail gracefully" by ensuring that compromise of one device does not compromise the entire system. In this manner, the attacker can be practically restricted to attacks that cost less than the expected return from compromising a single device (plus, perhaps, a little more for kudos). Since the most sophisticated attacks have been estimated to cost several hundred thousand dollars to carry out, carefully designed systems may be invulnerable in practice.

QUESTION 105
What kind of certificate is used to validate a user identity?

A. Public key certificate
B. Attribute certificate
C. Root certificate
D. Code signing certificate

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: In cryptography, a public key certificate (or identity certificate) is an electronic document which incorporates a digital signature to bind together a public key with an identity -- information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key

belongs to an individual. In a typical public key infrastructure (PKI) scheme, the signature will be of a certificate authority (CA). In a web of trust scheme, the signature is of either the user (a self-signed certificate) or other users ("endorsements"). In either case, the signatures on a certificate are attestations by the certificate signer that the identity information and the public key belong together. In computer security, an authorization certificate (also known as an attribute certificate) is a digital document that describes a written permission from the issuer to use a service or a resource that the issuer controls or has access to use. The permission can be delegated. Some people constantly confuse PKCs and ACs. An analogy may make the distinction clear. A PKC can be considered to be like a passport: it identifies the holder, tends to last for a long time, and should not be trivial to obtain. An AC is more like an entry visa: it is typically issued by a different authority and does not last for as long a time. As acquiring an entry visa typically requires presenting a passport, getting a visa can be a simpler process. A real life example of this can be found in the mobile software deployments by large service providers and are typically applied to platforms such as Microsoft Smartphone (and related), Symbian OS, J2ME, and others.
In each of these systems a mobile communications service provider may customize the mobile terminal client distribution (ie. the mobile phone operating system or application environment) to include one or more root certificates each associated with a set of capabilities or permissions such as "update firmware", "access address book", "use radio interface", and the most basic one, "install and execute". When a developer wishes to enable distribution and execution in one of these controlled environments they must acquire a certificate from an appropriate CA, typically a large commercial CA, and in the process they usually have their identity verified using out-of-band mechanisms such as a combination of phone call, validation of their legal entity through government and commercial databases, etc., similar to the high assurance SSL certificate vetting process, though often there are additional specific requirements imposed on would-be developers/publishers. Once the identity has been validated they are issued an identity certificate they can use to sign their software; generally the software signed by the developer or publisher's identity certificate is not distributed but rather it is submitted to processor to possibly test or profile the content before generating an authorization certificate which is unique to the particular software release. That certificate is then used with an ephemeral asymmetric key-pair to sign the software as the last step of preparation for distribution. There are many advantages to separating the identity and authorization certificates especially relating to risk mitigation of new content being accepted into the system and key management as well as recovery from errant software which can be used as attack vectors.

HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw-Hill/Osborne, page 540.
http://en.wikipedia.org/wiki/Attribute_certificate
http://en.wikipedia.org/wiki/Public_key_certificate

QUESTION 106
What does the directive of the European Union on Electronic Signatures deal with?

A. Encryption of classified data
B. Encryption of secret data
C. Non repudiation
D. Authentication of web servers

Correct Answer: C
Explanation

Explanation/Reference:
FORD, Warwick & BAUM, Michael S., Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption (2nd Edition), 2000, Prentice Hall PTR, Page 589; Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures.

QUESTION 107
A X.509 public key certificate with the key usage attribute "non repudiation" can be used for which of the following?

A. encrypting messages
B. signing messages

C. verifying signed messages
D. decrypt encrypted messages

Correct Answer: C
Explanation

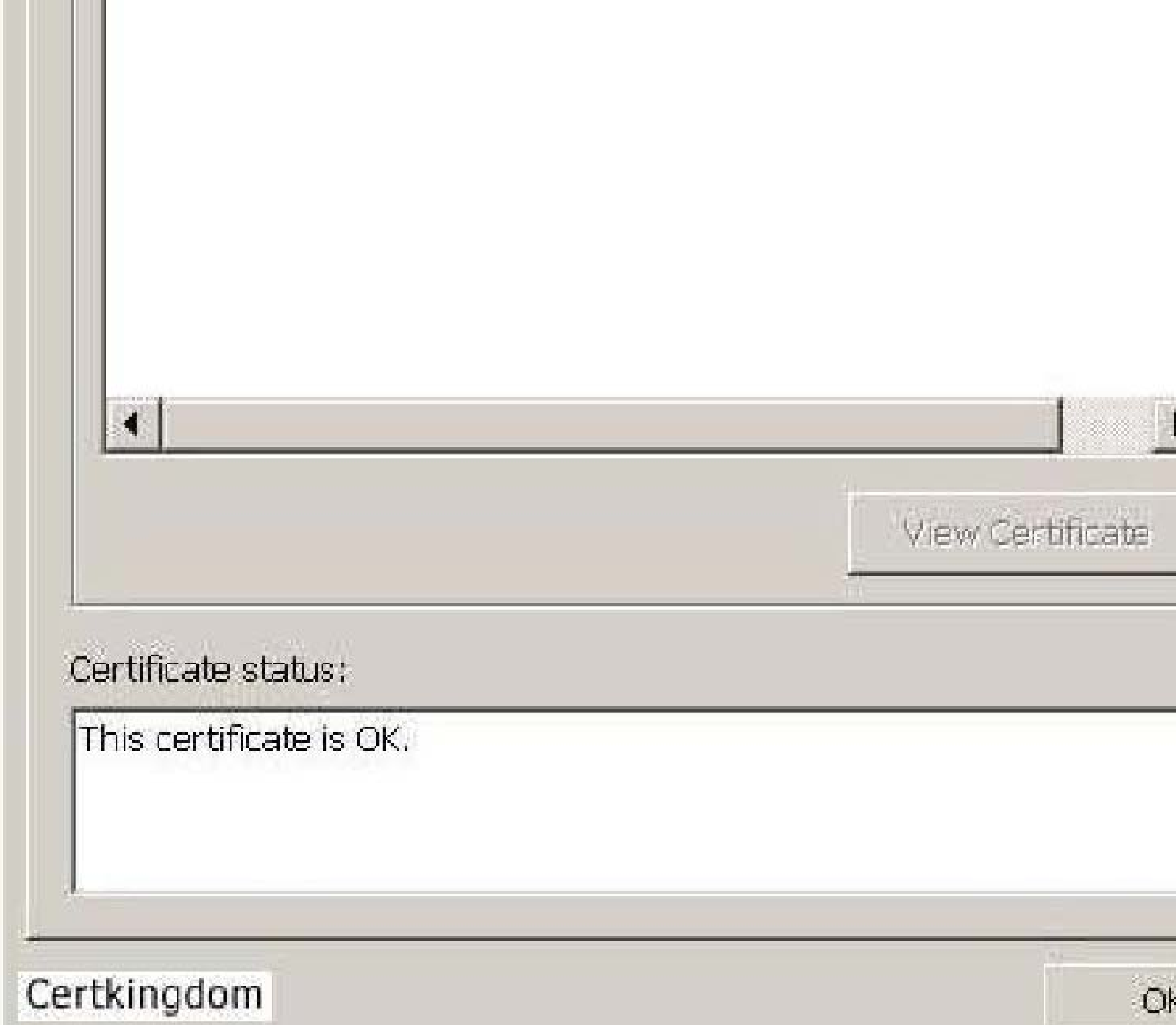
Explanation/Reference:
Explanation: RFC 2459 : Internet X.509 Public Key Infrastructure Certificate and CRL Profile; GUTMANN, P., X.509 style guide.

QUESTION 108
Which of the following would best describe certificate path validation?

A. Verification of the validity of all certificates of the certificate chain to the root certificate
B. Verification of the integrity of the associated root certificate
C. Verification of the integrity of the concerned private key
D. Verification of the revocation status of the concerned certificate

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: With the advent of public key cryptography (PKI), it is now possible to communicate securely with untrusted parties over the Internet without prior arrangement. One of the necessities arising from such communication is the ability to accurately verify someone's identity (i.e. whether the person you are communicating with is indeed the person who he/she claims to be). In order to be able to perform identity check for a given entity, there should be a fool-proof method of "binding" the entity's public key to its unique domain name (DN). A X.509 digital certificate issued by a well known certificate authority (CA), like Verisign, Entrust, Thawte, etc., provides a way of positively identifying the entity by placing trust on the CA to have performed the necessary verifications. A X.509 certificate is a cryptographically sealed data object that contains the entity's unique DN, public key, serial number, validity period, and possibly other extensions.
The Windows Operating System offers a Certificate Viewer utility which allows you to double-click on any certificate and review its attributes in a human-readable format. For instance, the "General" tab in the Certificate Viewer Window (see below) shows who the certificate was issued to as well as the certificate's issuer, validation period and usage functions.



Certification path:

VeriSign Class 3 Public Primary CA

www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 V

Certificate status:

This certificate is OK.

Certification Path graphic
The "Certification Path" tab contains the hierarchy for the chain of certificates. It allows you to select the certificate issuer or a subordinate certificate and then click on "View Certificate" to open the certificate in the Certificate Viewer.
Each end-user certificate is signed by its issuer, a trusted CA, by taking a hash value (MD5 or SHA-1) of ASN.1 DER (Distinguished Encoding Rule) encoded object and then encrypting the resulting hash with the issuer's private key (CA's Private Key) which is a digital signature. The encrypted data is stored in the "signatureValue" attribute of the entity's (CA) public certificate. Once the certificate is signed by the issuer, a party who wishes to communicate with this entity can then take the entity's public certificate and find out who the issuer of the certificate is. Once the issuer's of the certificate (CA) is identified, it would be possible to decrypt the value of the "signatureValue" attribute in the entity's certificate using the issuer's public key to retrieve thehash value. This hash value will be compared with the independently calculated hash on the entity's certificate. If the two hash values match, then the information contained within the certificate must not have been altered and, therefore, one must trust that the CA has done enough background check to ensure that all details in the entity's certificate are accurate. The process of cryptographically checking the signatures of all certificates in the certificate chain is called "key chaining". An additional check that is essential to key chaining is verifying that the value of the "subjectKeyIdentifier" extension in one certificate matches the same in the subsequent certificate.
Similarly, the process of comparing the subject field of the issuer certificate to the issuer field of the subordinate certificate is called "name chaining". In this process, these values must match for each pair of adjacent certificates in the certification path in order to guarantee that the path represents unbroken chain of entities relating directly to one another and that it has no missing links.
The two steps above are the steps to validate the Certification Path by ensuring the validity of all certificates of the certificate chain to the root certificate as described in the two paragraphs above.
Reference(s) used for this question:
FORD, Warwick & BAUM, Michael S., Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption (2nd Edition), 2000, Prentice Hall PTR, Page 262.
and
https://www.tibcommunity.com/docs/DOC-2197

QUESTION 109
Which of the following can best define the "revocation request grace period"?

A. The period of time allotted within which the user must make a revocation request upon a revocation reason
B. Minimum response time for performing a revocation by the CA
C. Maximum response time for performing a revocation by the CA
D. Time period between the arrival of a revocation request and the publication of the revocation information

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The length of time between the Issuer's receipt of a revocation request and the time the Issuer is required to revoke the certificate should bear a reasonable relationship to the amount of risk the participants are willing to assume that someone may rely on a certificate for which a proper evocation request has been given but has not yet been acted upon. How quickly revocation requests need to be processed (and CRLs or certificate status databases need to be updated) depends upon the specific application for which the Policy Authority is rafting the Certificate Policy.
A Policy Authority should recognize that there may be risk and lost tradeoffs with respect to grace periods for revocation notices.
If the Policy Authority determines that its PKI participants are willing to accept a grace period of a few hours in exchange for a lower implementation cost, the Certificate Policy may reflect that decision.

QUESTION 110
Which is NOT a suitable method for distributing certificate revocation information?

A. CA revocation mailing list

B. Delta CRL

C. OCSP (online certificate status protocol)

D. Distribution point CRL

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The following are incorrect answers because they are all suitable methods. A Delta CRL is a CRL that only provides information about certificates whose statuses have changed since the issuance of a specific, previously issued CRL. The Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate.
A Distribution point CRL or CRL Distribution Point, a location specified in the CRL Distribution Point (CRL DP) X.509, version 3, certificate extension when the certificate is issued.

RFC 2459: Internet X.509 Public Key Infrastru
http://csrc.nist.gov/groups/ST/crypto_apps_infra/documents/sliding_window.pdf http://www.ipswitch.eu/online_certificate_status_protocol_en.html Computer Security Handbook By Seymour Bosworth, Arthur E. Hutt, Michel E. Kabay http://books.google.com/books?id=rCx5OfSFUPkC&printsec=frontcover&dq=Computer+Security+ Handbook#PRA6-PA4,M1

QUESTION 111
Which of the following is true about digital certificate?

A. It is the same as digital signature proving Integrity and Authenticity of the data

B. Electronic credential proving that the person the certificate was issued to is who they claim to be

C. You can only get digital certificate from Verisign, RSA if you wish to prove the key belong to a specific user.

D. Can't contain geography data such as country for example.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Digital certificate helps others verify that the public keys presented by users are genuine and valid. It is a form of Electronic credential proving that the person the certificate was issued to is who they claim to be.
The certificate is used to identify the certificate holder when conducting electronic transactions. It is issued by a certification authority (CA). It contains the name of an organization or individual, the business address, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Some digital certificates conform to a standard, X.509. Digital certificates can be kept in registries so that authenticating users can look up other users' public keys.
Digital certificates are key to the PKI process. The digital certificate serves two roles. First, it ensures the integrity of the public key and makes sure that the key remains unchanged and in a valid state. Second, it validates that the public key is tied to the stated owner and that all associated information is true and correct. The information needed to accomplish these goals is added into the digital certificate.
A Certificate Authority (CA) is an entity trusted by one or more users as an authority in a network that issues, revokes, and manages digital certificates. A Registration Authority (RA) performs certificate registration services on behalf of a C A. The RA,
a single purpose server, is responsible for the accuracy of the information contained in a certificate request. The RA is also expected to perform user validation before issuing a certificate request. A Digital Certificate is not like same as a digital signature, they are two different things, a digital Signature is created by using your Private key to encrypt a message digest and a Digital Certificate is issued by a trusted third party who vouch for your identity. There are many other third parties which are providing Digital Certifictes and not just Verisign, RSA.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press)

(Kindle Locations 14894-14903). Auerbach Publications. Kindle Edition. Gregg, Michael; Haines, Billy (2012-02-16). CASP: CompTIA Advanced Security Practitioner Study Guide Authorized Courseware: Exam CAS-001 (p. 24). Wiley. Kindle Edition. Please refer to http://en.wikipedia.org/wiki/Digital_certificate What is Digital certificate:
http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211947,00.html another deifination on http://www.webopedia.com/TERM/D/digital_certificate.html

QUESTION 112
What kind of Encryption technology does SSL utilize?

A. Secret or Symmetric key
B. Hybrid (both Symmetric and Asymmetric)
C. Public Key
D. Private key

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: SSL use public-key cryptography to secure session key, while the session key (secret key) is used to secure the whole session taking place between both parties communicating with each other.
The SSL protocol was originally developed by Netscape. Version 1.0 was never publicly released; version 2.0 was released in February 1995 but "contained a number of security flaws which ultimately led to the design of SSL version 3.0." SSL version 3.0, released in 1996, was a complete redesign of the protocol produced by Paul Kocher working with Netscape engineers Phil Karlton and Alan Freier.
All of the other answers are incorrect

QUESTION 113
What is the name of a one way transformation of a string of characters into a usually shorter fixedlength value or key that represents the original string? Such a transformation cannot be reversed?

A. One-way hash
B. DES
C. Transposition
D. Substitution

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: A cryptographic hash function is a transformation that takes an input (or 'message') and returns a fixed-size string, which is called the hash value (sometimes termed a message digest, a digital fingerprint, a digest or a checksum). The ideal hash function has three main properties - it is extremely easy to calculate a hash for any given data, it is extremely difficult or almost impossible in a practical sense to calculate a text that has a given hash, and it is extremely unlikely that two different messages, however close, will have the same hash.
Functions with these properties are used as hash functions for a variety of purposes, both within and outside cryptography. Practical applications include message integrity checks, digital signatures, authentication, and various information security applications. A hash can also act as a concise representation of the message or document from which it was computed, and allows easy indexing of duplicate or unique data files.
In various standards and applications, the two most commonly used hash functions are MD5 and SHA-1. In 2005, security flaws were identified in both of these, namely that a possible mathematical weakness might exist, indicating that a stronger hash function would be desirable. In 2007 the National Institute of Standards and Technology announced a contest to design a hash function which will be given the name SHA-3 and be the subject of a FIPS standard. A hash function takes a string of any length as input and produces a fixed length string which acts as a kind of "signature" for the data provided. In this way, a person knowing the hash is unable to work out the original message, but someone knowing the original message can prove the hash is

created from that message, and none other. A cryptographic hash function should behave as much as possible like a random function while still being deterministic and efficiently computable. A cryptographic hash function is considered "insecure" from a cryptographic point of view, if either of the following is computationally feasible:
finding a (previously unseen) message that matches a given digest finding "collisions", wherein two different messages have the same message digest. An attacker who can do either of these things might, for example, use them to substitute an authorized message with an unauthorized one.
Ideally, it should not even be feasible to find two messages whose digests are substantially similar; nor would one want an attacker to be able to learn anything useful about a message given only its digest. Of course the attacker learns at least one piece of information, the digest itself, which for instance gives the attacker the ability to recognise the same message should it occur again.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 40-41.
also see:
http://en.wikipedia.org/wiki/Cryptographic_hash_function

QUESTION 114
Which of the following is NOT an asymmetric key algorithm?

A. RSA
B. Elliptic Curve Cryptosystem (ECC)
C. El Gamal
D. Data Encryption System (DES)

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Data Encryption Standard (DES) is a symmetric key algorithm. Originally developed by IBM, under project name Lucifer, this 128-bit algorithm was accepted by the NIST in 1974, but the key size was reduced to 56 bits, plus 8 bits for parity. It somehow became a national cryptographic standard in 1977, and an American National Standard Institute (ANSI) standard in 1978. DES was later replaced by the Advanced Encryption Standard (AES) by the NIST. All other options are asymmetric algorithms.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 8: Cryptography (page 525).
DES: http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

QUESTION 115
Which of the following is NOT a symmetric key algorithm?

A. Blowfish
B. Digital Signature Standard (DSS)
C. Triple DES (3DES)
D. RC5

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Digital Signature Standard (DSS) specifies a Digital Signature Algorithm (DSA) appropriate for applications requiring a digital signature, providing the capability to generate signatures (with the use of a private key) and verify them (with the use of the corresponding public key).
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 8: Cryptography (page 550).
DSS: http://www.itl.nist.gov/fipspubs/fip186.htm.

QUESTION 116
Which of the following ASYMMETRIC encryption algorithms is based on the difficulty of FACTORING LARGE NUMBERS?

A. El Gamal
B. Elliptic Curve Cryptosystems (ECCs)
C. RSA
D. International Data Encryption Algorithm (IDEA)

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Named after its inventors Ron Rivest , Adi Shamir and Leonard Adleman is based on the difficulty of factoring large prime numbers.
Factoring a number means representing it as the product of prime numbers. Prime numbers, such as 2, 3, 5, 7, 11, and 13, are those numbers that are not evenly divisible by any smaller number, except 1. A non-prime, or composite number, can be written as the product of smaller primes, known as its prime factors. 665, for example is the product of the primes 5, 7, and 19. A number is said to be factored when all of its prime factors are identified. As the size of the number increases, the difficulty of factoring increases rapidly.
The other answers are incorrect because:
El Gamal is based on the discrete logarithms in a finite field. Elliptic Curve Cryptosystems (ECCs) computes discrete logarithms of elliptic curves. International Data Encryption Algorithm (IDEA) is a block cipher and operates on 64 bit blocks of data and is a SYMMETRIC algorithm.
Reference : Shon Harris , AIO v3 , Chapter-8 : Cryptography , Page : 638

QUESTION 117
The Diffie-Hellman algorithm is primarily used to provide which of the following?

A. Confidentiality
B. Key Agreement
C. Integrity
D. Non-repudiation

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Diffie and Hellman describe a means for two parties to agree upon a shared secret in such a way that the secret will be unavailable to eavesdroppers. This secret may then be converted into cryptographic keying material for other (symmetric) algorithms. A large number of minor variants of this process exist. See RFC 2631 Diffie-Hellman Key Agreement Method for more details.
In 1976, Diffie and Hellman were the first to introduce the notion of public key cryptography, requiring a system allowing the exchange of secret keys over non-secure channels. The Diffie- Hellman algorithm is used for key exchange between two parties communicating with each other, it cannot be used for encrypting and decrypting messages, or digital signature. Diffie and Hellman sought to address the issue of having to exchange keys via courier and other unsecure means. Their efforts were the FIRST asymmetric key agreement algorithm. Since the Diffie-Hellman algorithm cannot be used for encrypting and decrypting it cannot provide confidentiality nor integrity. This algorithm also does not provide for digital signature functionality and thus non-repudiation is not a choice.
NOTE: The DH algorithm is susceptible to man-in-the-middle attacks.
KEY AGREEMENT VERSUS KEY EXCHANGE
A key exchange can be done multiple way. It can be done in person, I can generate a key and then encrypt the key to get it securely to you by encrypting it with your public key. A Key Agreement protocol is done over a public medium such as the internet using a mathematical formula to come out with a common value on both sides of the communication link, without the ennemy being able to know what the common agreement is.
The following answers were incorrect:

All of the other choices were not correct choices
Reference(s) used for this question:
Shon Harris, CISSP All In One (AIO), 6th edition . Chapter 7, Cryptography, Page 812. http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange http://www.google.com/patents?vid=4200770

QUESTION 118
Which protocol makes USE of an electronic wallet on a customer's PC and sends encrypted credit card information to merchant's Web server, which digitally signs it and sends it on to its processing bank?

A. SSH (Secure Shell)
B. S/MIME (Secure MIME)
C. SET (Secure Electronic Transaction)
D. SSL (Secure Sockets Layer)

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: As protocol was introduced by Visa and Mastercard to allow for more credit card transaction possibilities. It is comprised of three different pieces of software, running on the customer's PC (an electronic wallet), on the merchant's Web server and on the payment server of the merchant's bank. The credit card information is sent by the customer to the merchant's Web server, but it does not open it and instead digitally signs it and sends it to its bank's payment server for processing.
The following answers are incorrect because :
SSH (Secure Shell) is incorrect as it functions as a type of tunneling mechanism that provides terminal like access to remote computers.
S/MIME is incorrect as it is a standard for encrypting and digitally signing electronic mail and for providing secure data transmissions.
SSL is incorrect as it uses public key encryption and provides data encryption, server authentication, message integrity, and optional client authentication. Reference : Shon Harris AIO v3 , Chapter-8: Cryptography , Page : 667-669

QUESTION 119
Which of the following algorithms does NOT provide hashing?

A. SHA-1
B. MD2
C. RC4
D. MD5

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: As it is an algorithm used for encryption and does not provide hashing functions , it is also commonly implemented ' Stream Ciphers '.
The other answers are incorrect because :
SHA-1 was designed by NIST and NSA to be used with the Digital Signature Standard (DSS). SHA was designed to be used in digital signatures and was developed when a more secure hashing algorithm was required for U.S. government applications. MD2 is a one-way hash function designed by Ron Rivest that creates a 128-bit message digest value. It is not necessarily any weaker than the other algorithms in the "MD" family, but it is much slower.
MD5 was also created by Ron Rivest and is the newer version of MD4. It still produces a 128-bit hash, but the algorithm is more complex, which makes it harder to break. Reference : Shon Harris , AIO v3 , Chapter - 8 : Cryptography , Page : 644 - 645

QUESTION 120

In what type of attack does an attacker try, from several encrypted messages, to figure out the key used in the encryption process?

A. Known-plaintext attack
B. Ciphertext-only attack
C. Chosen-Ciphertext attack
D. Plaintext-only attack

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: In a ciphertext-only attack, the attacker has the ciphertext of several messages encrypted with the same encryption algorithm. Its goal is to discover the plaintext of the messages by figuring out the key used in the encryption process. In a known-plaintext attack, the attacker has the plaintext and the ciphertext of one or more messages. In a chosen-ciphertext attack, the attacker can chose the ciphertext to be decrypted and has access to the resulting plaintext. Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 8: Cryptography (page 578).

QUESTION 121
Which encryption algorithm is BEST suited for communication with handheld wireless devices?

A. ECC (Elliptic Curve Cryptosystem)
B. RSA
C. SHA
D. RC4

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: As it provides much of the same functionality that RSA provides: digital signatures, secure key distribution,and encryption. One differing factor is ECC's efficiency. ECC is more efficient that RSA and any other asymmetric algorithm.
The following answers are incorrect because :
RSA is incorrect as it is less efficient than ECC to be used in handheld devices.
SHA is also incorrect as it is a hashing algorithm.
RC4 is also incorrect as it is a symmetric algorithm.
Reference : Shon Harris AIO v3 , Chapter-8 : Cryptography , Page : 631 , 638.

QUESTION 122
Which of the following keys has the SHORTEST lifespan?

A. Secret key
B. Public key
C. Session key
D. Private key

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: As session key is a symmetric key that is used to encrypt messages between two users. A session key is only good for one communication session between users. For example , If Tanya has a symmetric key that she uses to encrypt messages between Lance and herself all the time , then this symmetric key would not be regenerated or changed. They would use the same key every time they communicated using

encryption. However , using the same key repeatedly increases the chances of the key being captured and the secure communication being compromised. If , on the other hand , a new symmetric key were generated each time Lance and Tanya wanted to communicate , it would be used only during their dialog and then destroyed. if they wanted to communicate and hour later , a new session key would be created and shared.
The other answers are not correct because :
Public Key can be known to anyone.
Private Key must be known and used only by the owner.
Secret Keys are also called as Symmetric Keys, because this type of encryption relies on each user to keep the key a secret and properly protected.

SHON HARRIS , ALL IN ONE THIRD EDITION : Chapter 8 : Cryptography , Page : 619-620

QUESTION 123
What is the RESULT of a hash algorithm being applied to a message ?

A. A digital signature
B. A ciphertext
C. A message digest
D. A plaintext

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: As when a hash algorithm is applied on a message , it produces a message digest.
The other answers are incorrect because :
A digital signature is a hash value that has been encrypted with a sender's private key. A ciphertext is a message that appears to be unreadable.
A plaintext is a readable data.
Reference : Shon Harris , AIO v3 , Chapter-8 : Cryptography , Page : 593-594 , 640 , 648

QUESTION 124
Secure Sockets Layer (SSL) uses a Message Authentication Code (MAC) for what purpose?

A. message non-repudiation.
B. message confidentiality.
C. message interleave checking.
D. message integrity.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: A keyed hash also called a MAC (message authentication code) is used for integrity protection and authenticity.
In cryptography, a message authentication code (MAC) is a generated value used to authenticate a message. A MAC can be generated by HMAC or CBC-MAC methods. The MAC protects both a message's integrity (by ensuring that a different MAC will be produced if the message has changed) as well as its authenticity, because only someone who knows the secret key could have modified the message.
MACs differ from digital signatures as MAC values are both generated and verified using the same secret key. This implies that the sender and receiver of a message must agree on the same key before initiating communications, as is the case with symmetric encryption. For the same reason, MACs do not provide the property of non-repudiation offered by signatures specifically in the case of a network-wide shared secret key: any user who can verify a MAC is also capable of generating MACs for other messages.
HMAC
When using HMAC the symmetric key of the sender would be concatenated (added at the end) with the message. The result of this process (message + secret key) would be put through a hashing algorithm, and the

result would be a MAC value. This MAC value is then appended to the message being sent. If an enemy were to intercept this message and modify it, he would not have the necessary symmetric key to create a valid MAC value. The receiver would detect the tampering because the MAC value would not be valid on the receiving side.

CBC-MAC

If a CBC-MAC is being used, the message is encrypted with a symmetric block cipher in CBC mode, and the output of the final block of ciphertext is used as the MAC. The sender does not send the encrypted version of the message, but instead sends the plaintext version and the MAC attached to the message. The receiver receives the plaintext message and encrypts it with the same symmetric block cipher in CBC mode and calculates an independent MAC value. The receiver compares the new MAC value with the MAC value sent with the message. This method does not use a hashing algorithm as does HMAC.

Cipher-Based Message Authentication Code (CMAC)

Some security issues with CBC-MAC were found and they created Cipher-Based Message Authentication Code (CMAC) as a replacement. CMAC provides the same type of data origin authentication and integrity as CBC-MAC, but is more secure mathematically. CMAC is a variation of CBC-MAC. It is approved to work with AES and Triple DES. HMAC, CBC-MAC, and CMAC work higher in the network stack and can identify not only transmission errors (accidental), but also more nefarious modifications, as in an attacker messing with a message for her own benefit. This means all of these technologies can identify intentional, unauthorized modifications and accidental changes-- three in one.

The following are all incorrect answers:

"Message non-repudiation" is incorrect.

Nonrepudiation is the assurance that someone cannot deny something. Typically, nonrepudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated. To repudiate means to deny. For many years, authorities have sought to make repudiation impossible in some situations. You might send registered mail, for example, so the recipient cannot deny that a letter was delivered. Similarly, a legal document typically requires witnesses to signing so that the person who signs cannot deny having done so. On the Internet, a digital signature is used not only to ensure that a message or document has been electronically signed by the person that purported to sign the document, but also, since a digital signature can only be created by one person, to ensure that a person cannot later deny that they furnished the signature.

"Message confidentiality" is incorrect. The Message confidentiality is protected by encryption not by hashing algorithms.

"Message interleave checking" is incorrect. This is a nonsense term included as a distractor.

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 1384). McGraw-Hill.
Kindle Edition.
and
http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf and
http://searchsecurity.techtarget.com/definition/nonrepudiation and
https://en.wikipedia.org/wiki/Message_authentication_code

QUESTION 125

Which of the following services is NOT provided by the digital signature standard (DSS)?

A. Encryption
B. Integrity
C. Digital signature
D. Authentication

Correct Answer: A
Explanation

Explanation/Reference:

Explanation: DSS provides Integrity, digital signature and Authentication, but does not provide Encryption.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 160).

QUESTION 126

What can be defined as an instance of two different keys generating the same ciphertext from the same plaintext?

A. Key collision
B. Key clustering
C. Hashing
D. Ciphertext collision

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Key clustering happens when a plaintext message generates identical ciphertext messages using the same transformation algorithm, but with different keys. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 130).

QUESTION 127
Which of the following is true about link encryption?

A. Each entity has a common key with the destination node.
B. Encrypted messages are only decrypted by the final node.
C. This mode does not provide protection if anyone of the nodes along the transmission path is compromised.
D. Only secure nodes are used in this type of transmission.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: In link encryption, each entity has keys in common with its two neighboring nodes in the transmission chain.
Thus, a node receives the encrypted message from its predecessor, decrypts it, and then reencrypts it with a new key, common to the successor node. Obviously, this mode does not provide protection if anyone of the nodes along the transmission path is compromised. Encryption can be performed at different communication levels, each with different types of protection and implications. Two general modes of encryption implementation are link encryption and end-to-end encryption.
Link encryption encrypts all the data along a specific communication path, as in a satellite link, T3 line, or telephone circuit. Not only is the user information encrypted, but the header, trailers, addresses, and routing data that are part of the packets are also encrypted. The only traffic not encrypted in this technology is the data link control messaging information, which includes instructions and parameters that the different link devices use to synchronize communication methods. Link encryption provides protection against packet sniffers and eavesdroppers. In end-to-end encryption, the headers, addresses, routing, and trailer information are not encrypted, enabling attackers to learn more about a captured packet and where it is headed.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (pp. 845-846). McGraw-Hill.
And:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 132).

QUESTION 128
What uses a key of the same length as the message where each bit or character from the plaintext is encrypted by a modular addition?

A. Running key cipher
B. One-time pad
C. Steganography

D. Cipher block chaining

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: In cryptography, the one-time pad (OTP) is a type of encryption that is impossible to crack if used correctly. Each bit or character from the plaintext is encrypted by a modular addition with a bit or character from a secret random key (or pad) of the same length as the plaintext, resulting in a ciphertext. If the key is truly random, at least as long as the plaintext, never reused in whole or part, and kept secret, the ciphertext will be impossible to decrypt or break without knowing the key. It has also been proven that any cipher with the perfect secrecy property must use keys with effectively the same requirements as OTP keys. However, practical problems have prevented one-time pads from being widely used.
First described by Frank Miller in 1882, the one-time pad was re-invented in 1917 and patented a couple of years later. It is derived from the Vernam cipher, named after Gilbert Vernam, one of its inventors. Vernam's system was a cipher that combined a message with a key read from a punched tape. In its original form, Vernam's system was vulnerable because the key tape was a loop, which was reused whenever the loop made a full cycle. One-time use came a little later when Joseph Mauborgne recognized that if the key tape were totally random, cryptanalysis would be impossible.
The "pad" part of the name comes from early implementations where the key material was distributed as a pad of paper, so the top sheet could be easily torn off and destroyed after use. For easy concealment, the pad was sometimes reduced to such a small size that a powerful magnifying glass was required to use it. Photos show captured KGB pads that fit in the palm of one's hand, or in a walnut shell. To increase security, one-time pads were sometimes printed onto sheets of highly flammable nitrocellulose so they could be quickly burned.
The following are incorrect answers:
A running key cipher uses articles in the physical world rather than an electronic algorithm. In classical cryptography, the running key cipher is a type of polyalphabetic substitution cipher in which a text, typically from a book, is used to provide a very long keystream. Usually, the book to be used would be agreed ahead of time, while the passage to use would be chosen randomly for each message and secretly indicated somewhere in the message. The Running Key cipher has the same internal workings as the Vigenere cipher. The difference lies in how the key is chosen; the Vigenere cipher uses a short key that repeats, whereas the running key cipher uses a long key such as an excerpt from a book. This means the key does not repeat, making cryptanalysis more difficult. The cipher can still be broken though, as there are statistical patterns in both the key and the plaintext which can be exploited. Steganography is a method where the very existence of the message is concealed. It is the art and science of encoding hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. it is sometimes referred to as Hiding in Plain Sight.
Cipher block chaining is a DES operating mode. IBM invented the cipher-block chaining (CBC) mode of operation in 1976. In CBC mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block depends on all plaintext blocks processed up to that point. To make each message unique, an initialization vector must be used in the first block.
Reference(s) used for this question:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter
8: Cryptography (page 555).
and
http://en.wikipedia.org/wiki/One-time_pad
http://en.wikipedia.org/wiki/Running_key_cipher
http://en.wikipedia.org/wiki/Cipher_block_chaining#Cipher-block_chaining_.28CBC.29

QUESTION 129
What can be defined as secret communications where the very existence of the message is hidden?

A. Clustering
B. Steganography
C. Cryptology
D. Vernam cipher

Correct Answer: B

Explanation

Explanation/Reference:
Explanation: Steganography is a secret communication where the very existence of the message is hidden. For example, in a digital image, the least significant bit of each word can be used to comprise a message without causing any significant change in the image. Key clustering is a situation in which a plaintext message generates identical ciphertext messages using the same transformation algorithm but with different keys. Cryptology encompasses cryptography and cryptanalysis. The Vernam Cipher, also called a one-time pad, is an encryption scheme using a random key of the same size as the message and is used only once. It is said to be unbreakable, even with infinite resources.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 134).

QUESTION 130
What is the maximum number of different keys that can be used when encrypting with Triple DES?

A. 1
B. 2
C. 3
D. 4

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Triple DES encrypts a message three times. This encryption can be accomplished in several ways. The most secure form of triple DES is when the three encryptions are performed with three different keys.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 152).

QUESTION 131
What algorithm has been selected as the AES algorithm, replacing the DES algorithm?

A. RC6
B. Twofish
C. Rijndael
D. Blowfish

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: On October 2, 2000, NIST announced the selection of the Rijndael Block Cipher, developed by the Belgian cryptographers Dr. Joan Daemen and Dr. Vincent Rijmen, as the proposed AES algorithm. Twofish and RC6 were also candidates. Blowfish is also a symmetric algorithm but wasn't a finalist for a replacement for DES. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 152).

QUESTION 132
Which of the following is a symmetric encryption algorithm?

A. RSA
B. Elliptic Curve
C. RC5
D. El Gamal

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: RC5 is a symmetric encryption algorithm. It is a block cipher of variable block length, encrypts through integer addition, the application of a bitwise Exclusive OR (XOR), and variable rotations.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 153).

QUESTION 133
Which of the following is NOT a property of the Rijndael block cipher algorithm?

A. The key sizes must be a multiple of 32 bits
B. Maximum block size is 256 bits
C. Maximum key size is 512 bits
D. The key size does not have to match the block size

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The above statement is NOT true and thus the correct answer. The maximum key size on Rijndael is 256 bits.
There are some differences between Rijndael and the official FIPS-197 specification for AES. Rijndael specification per se is specified with block and key sizes that must be a multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits. Namely, Rijndael allows for both key and block sizes to be chosen independently from the set of { 128, 160, 192, 224, 256 } bits. (And the key size does not in fact have to match the block size). However, FIPS-197 specifies that the block size must always be 128 bits in AES, and that the key size may be either 128, 192, or 256 bits. Therefore AES-128, AES-192, and AES-256 are actually:

	Key Size (bits)	Block Size (bits)
AES-128	128	128
AES-192	192	128
AES-256	256	128

So in short:
Rijndael and AES differ only in the range of supported values for the block length and cipher key length.
For Rijndael, the block length and the key length can be independently specified to any multiple of 32 bits, with a minimum of 128 bits, and a maximum of 256 bits. AES fixes the block length to 128 bits, and supports key lengths of 128, 192 or 256 bits only.
References used for this question:
http://blogs.msdn.com/b/shawnfa/archive/2006/10/09/the-differences-between-rijndael-andaes.
aspx
and
http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael.pdf

QUESTION 134
Which of the following is not a property of the Rijndael block cipher algorithm?

A. It employs a round transformation that is comprised of three layers of distinct and invertible transformations.
B. It is suited for high speed chips with no area restrictions.
C. It operates on 64-bit plaintext blocks and uses a 128 bit key.
D. It could be used on a smart card.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: All other properties above apply to the Rijndael algorithm, chosen as the AES standard to replace DES.
The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. Rijndael was designed to handle additional block sizes and key lengths, however they are not adopted in the AES standard. IDEA cipher algorithm operates on 64-bit plaintext blocks and uses a 128 bit key.
Reference(s) used for this question:
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf and
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

QUESTION 135

What is the maximum allowable key size of the Rijndael encryption algorithm?

A. 128 bits
B. 192 bits
C. 256 bits
D. 512 bits

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The Rijndael algorithm, chosen as the Advanced Encryption Standard (AES) to replace DES, can be categorized as an iterated block cipher with a variable block length and key length that can be independently chosen as 128, 192 or 256 bits. Below you have a summary of the differences between AES and Rijndael. AES is the advanced encryption standard defined by FIPS 197. It is implemented differently than Rijndael:
FIPS-197 specifies that the block size must always be 128 bits in AES, and that the key size may be either 128, 192, or 256 bits. Therefore AES-128, AES-192, and AES-256 are actually:
Key Size (bits) Number of rounds
Block Size (bits)
AES-128
128 10 Rounds
AES-192
192 12 Rounds
AES-256
256 14 Rounds
Some book will say "up to 9 rounds will be done with a 128 bits keys". Really it is 10 rounds because you must include round zero which is the first round. By contrast, the Rijndael specification per se is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 153).
and
FIPS 197
and
https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

QUESTION 136

Which of the following algorithms is used today for encryption in PGP?

A. RSA
B. IDEA
C. Blowfish
D. RC5

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The Pretty Good Privacy (PGP) email encryption system was developed by Phil Zimmerman. For encrypting messages, it actually uses AES with up to 256-bit keys, CAST, TripleDES, IDEA and Twofish. RSA is also used in PGP, but only for symmetric key exchange and for digital signatures, but not for encryption.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (pages 154, 169).
More info on PGP can be found on their site at http://www.pgp.com/display.php?pageID=29.

QUESTION 137
Which of the following protects Kerberos against replay attacks?

A. Tokens
B. Passwords
C. Cryptography
D. Time stamps

Correct Answer: D
Explanation

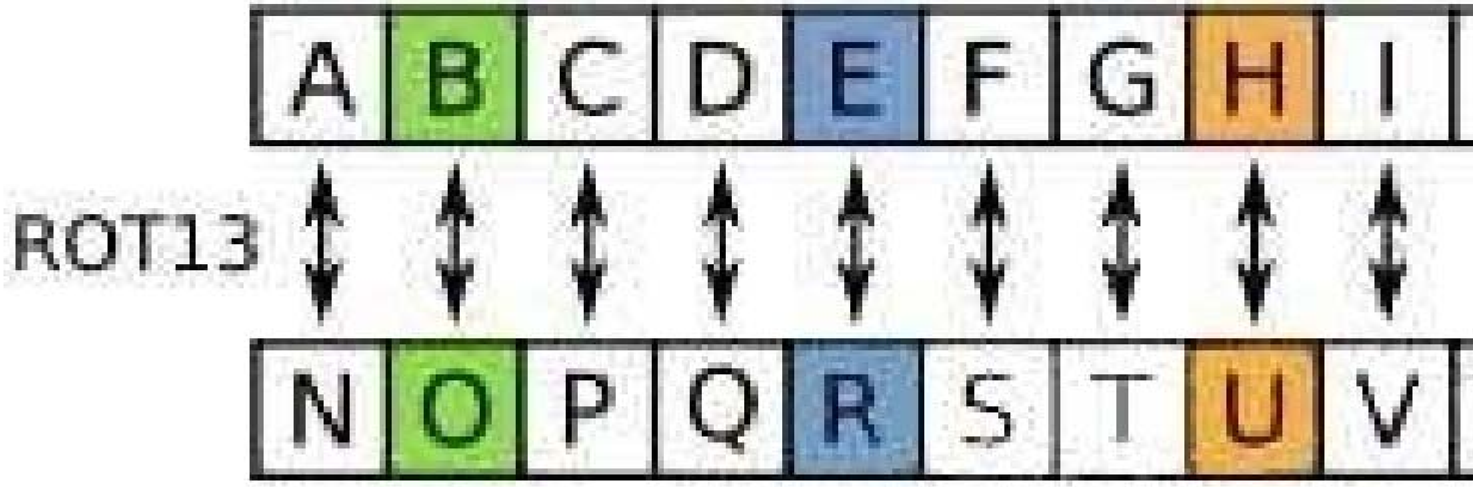
Explanation/Reference:
Explanation: A replay attack refers to the recording and retransmission of packets on the network. Kerberos uses time stamps, which protect against this type of attack. Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 8: Cryptography (page 581).

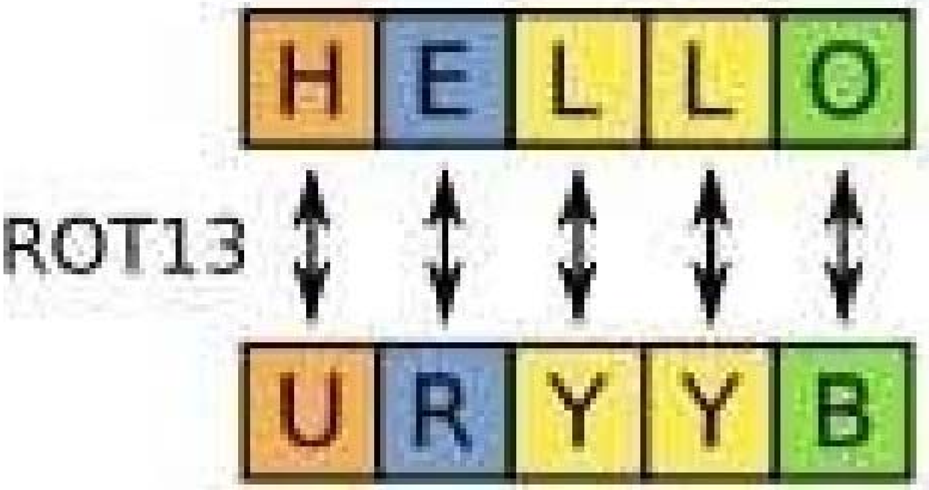
QUESTION 138
What is the name for a substitution cipher that shifts the alphabet by 13 places?

A. Caesar cipher
B. Polyalphabetic cipher
C. ROT13 cipher
D. Transposition cipher

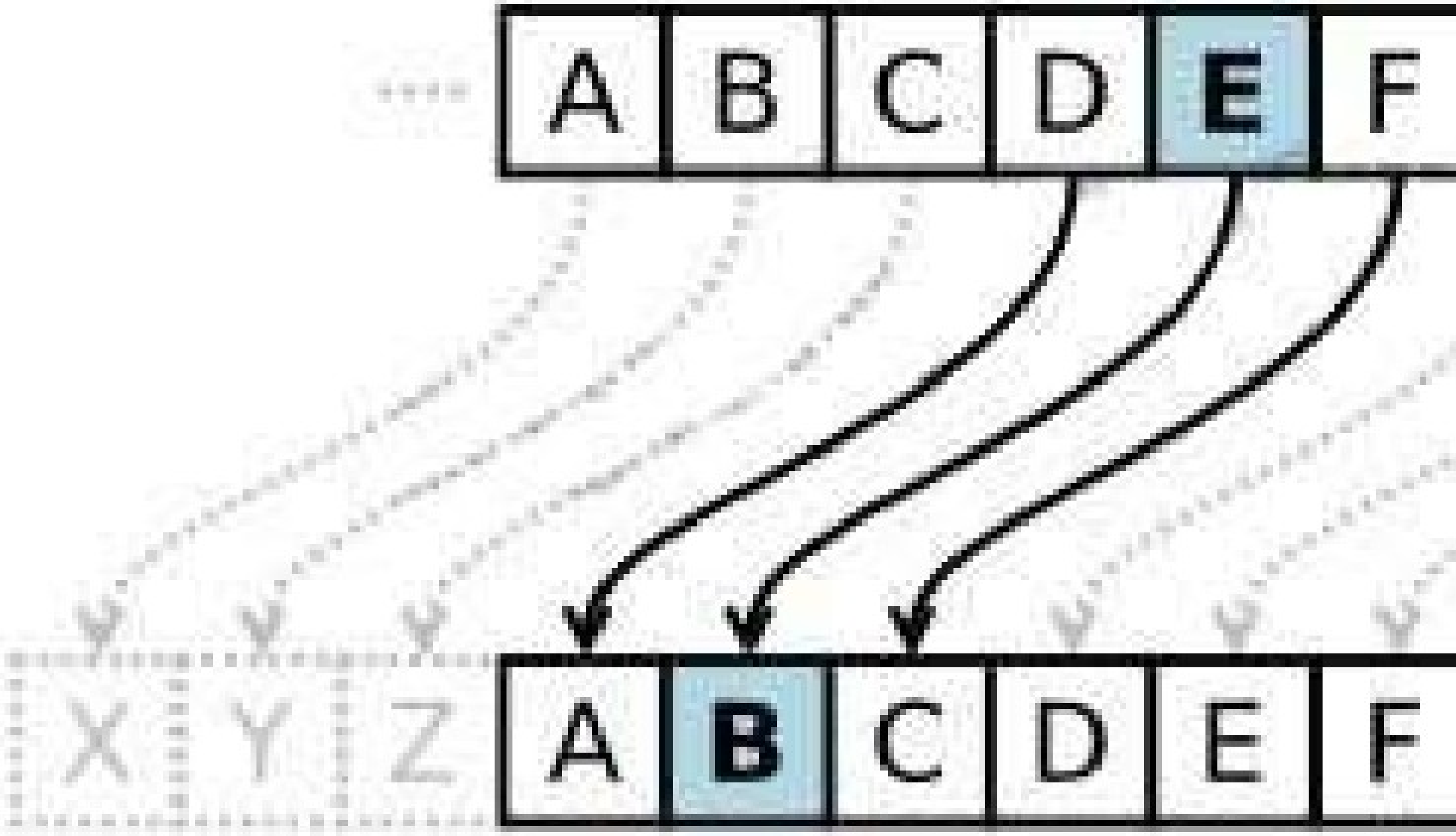
Correct Answer: C
Explanation

Explanation/Reference:
Explanation: An extremely simple example of conventional cryptography is a substitution cipher. A substitution cipher substitutes one piece of information for another. This is most frequently done by offsetting letters of the alphabet. Two examples are Captain Midnight's Secret Decoder Ring, which you may have owned when you were a kid, and Julius Caesar's cipher. In both cases, the algorithm is to offset the alphabet and the key is the number of characters to offset it. So the offset could be one, two, or any number you wish. ROT-13 is an example where it is shifted 13 spaces. The Ceaser Cipher is another example where it is shifted 3 letters to the left. ROT13 ("rotate by 13 places", sometimes hyphenated ROT-13) is a simple letter substitution cipher that replaces a letter with the letter 13 letters after it in the alphabet. ROT13 is an example of the Caesar cipher, developed in ancient Rome.
In the basic Latin alphabet, ROT13 is its own inverse; that is, to undo ROT13, the same algorithm is applied, so the same action can be used for encoding and decoding. The algorithm provides virtually no cryptographic security, and is often cited as a canonical example of weak encryption. ROT13 is used in online forums as a means of hiding spoilers, puzzle solutions, and offensive materials from the casual glance. ROT13 has been described as the "Usenet equivalent of a magazine printing the answer to a quiz upside down". ROT13 has inspired a variety of letter and word games on-line, and is frequently mentioned in newsgroup conversations.
See diagram Below:



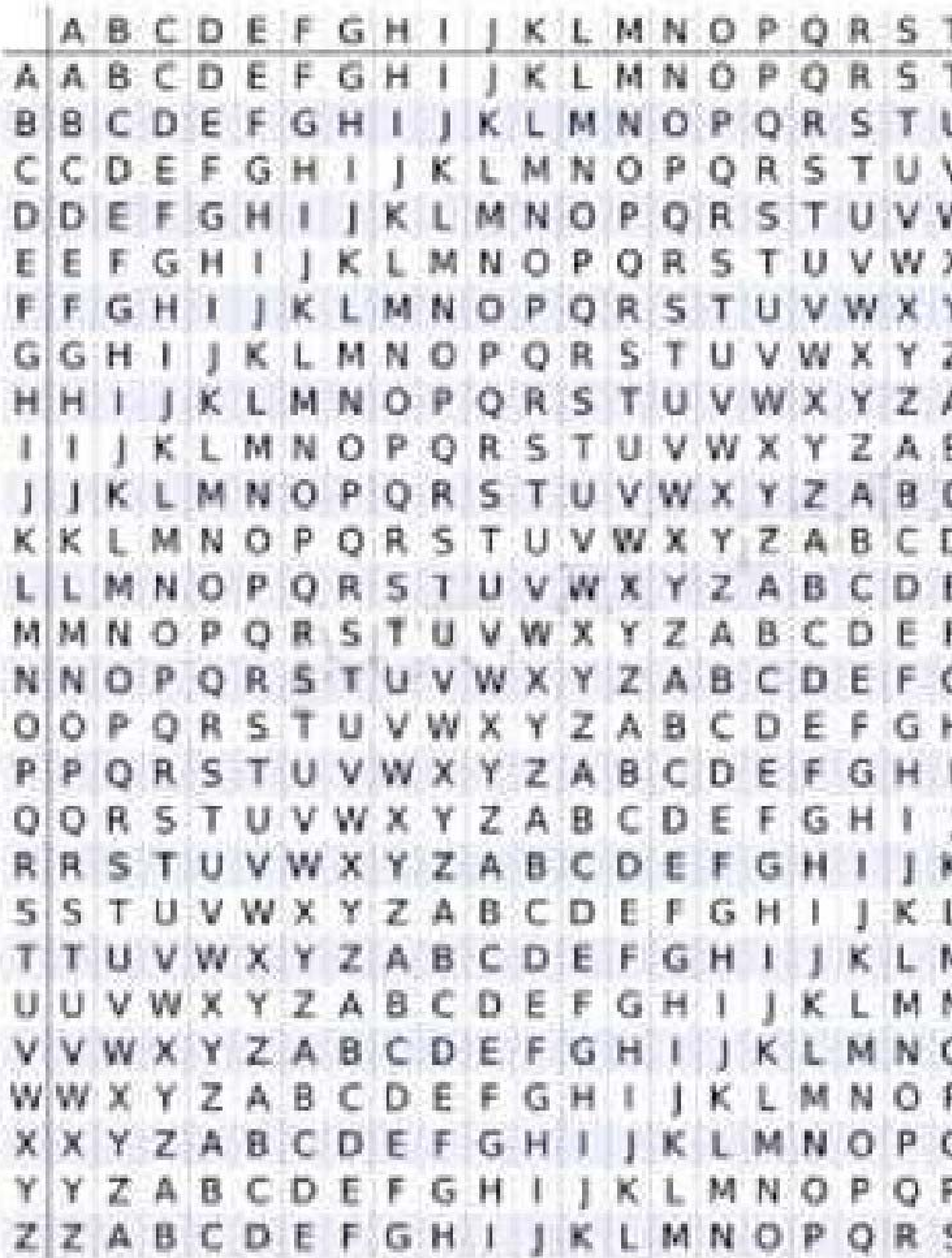


Rot 13 Cipher
The following are incorrect:
The Caesar cipher is a simple substitution cipher that involves shifting the alphabet three positions to the right. In cryptography, a Caesar cipher, also known as Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a left shift of 3, D would be replaced by A, E would become B, and so on. The method is named after Julius Caesar, who used it in his private correspondence.



Caesar Cipher

Polyalphabetic cipher refers to using multiple alphabets at a time. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The Vigenère cipher is probably the best-known example of a polyalphabetic cipher, though it is a simplified special case.

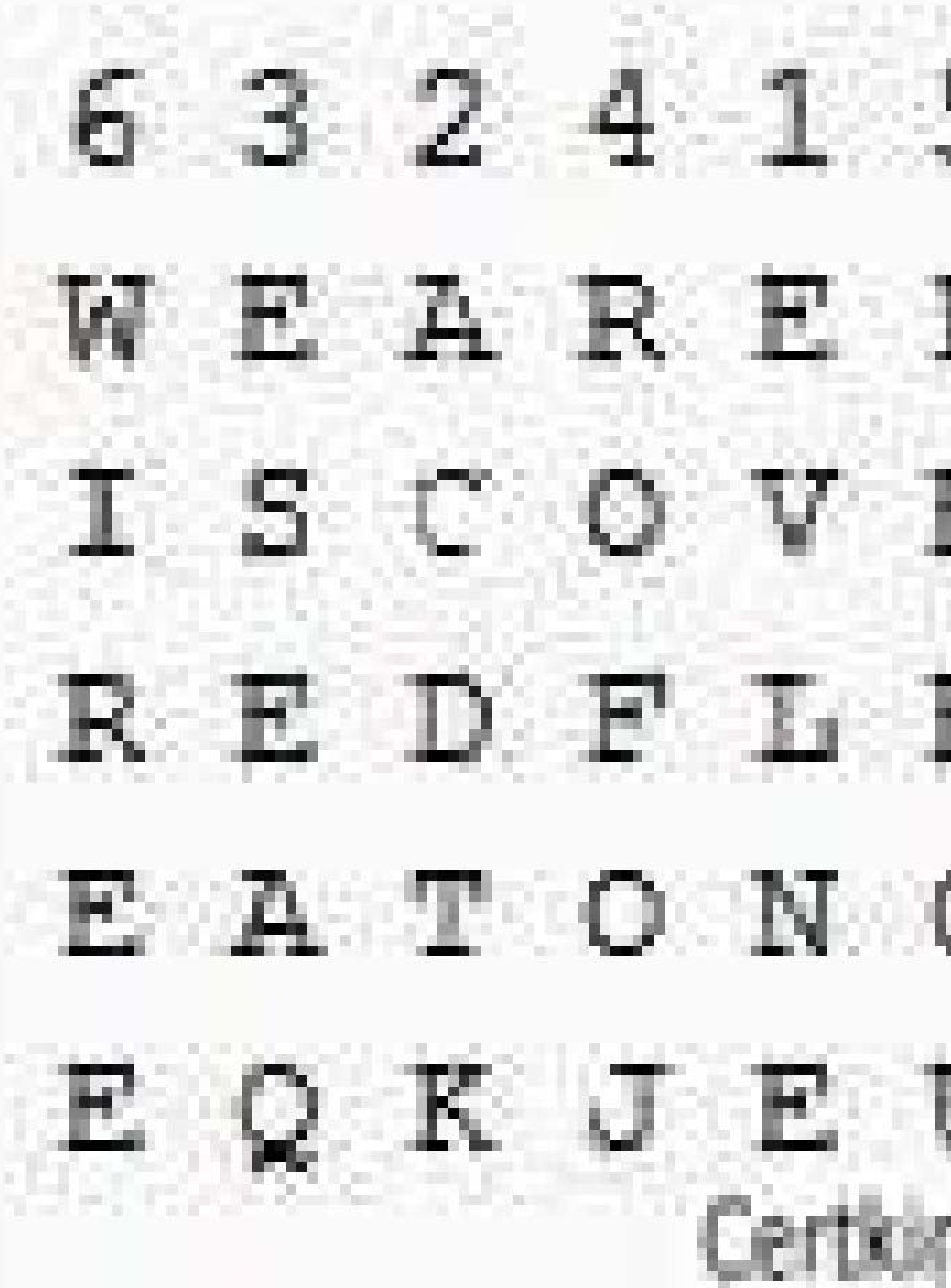


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S

Viginere Cipher

Transposition cipher is a different type of cipher. In cryptography, a transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext. That is, the order of the units is changed. See the reference below for multiple examples of Transpositio Ciphers. An exemple of Transposition cipher could be columnar transposition, the message is written out in rows of a fixed length, and then read out again column by column, and the columns are chosen in some scrambled order. Both the width of the rows and the permutation of the columns are usually defined by a keyword. For example, the word ZEBRAS is of length 6 (so the rows are of length 6), and the permutation is defined by the alphabetical order of the letters in the keyword. In this case, the order would be "6 3 2 4 1 5".

In a regular columnar transposition cipher, any spare spaces are filled with nulls; in an irregular columnar transposition cipher, the spaces are left blank. Finally, the message is read off in columns, in the order specified by the keyword. For example, suppose we use the keyword ZEBRAS and the message WE ARE DISCOVERED. FLEE AT ONCE. In a regular columnar transposition, we write this into the grid as Follows:



6	3	2	4	1
W	E	A	R	E
I	S	C	O	V
R	E	D	F	L
E	A	T	O	N
E	Q	K	J	E

Transposition Cipher
Providing five nulls (QKJEU) at the end. The ciphertext is then read off as:
EVLNE ACDTK ESEAQ ROFOJ DEECU WIREE
Reference(s) used for this question:
http://en.wikipedia.org/wiki/ROT13
http://en.wikipedia.org/wiki/Caesar_cipher
http://en.wikipedia.org/wiki/Polyalphabetic_cipher
http://en.wikipedia.org/wiki/Transposition_cipher

QUESTION 139
Which of the following standards concerns digital certificates?

A. X.400
B. X.25
C. X.509
D. X.75

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: X.509 is used in digital certificates. X.400 is used in e-mail as a message handling protocol. X.25 is a standard for the network and data link levels of a communication network and X.75 is a standard defining ways of connecting two X.25 networks. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 164).

QUESTION 140
Which of the following offers security to wireless communications?

A. S-WAP
B. WTLS
C. WSP
D. WDP

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Wireless Transport Layer Security (WTLS) is a communication protocol that allows wireless devices to send and receive encrypted information over the Internet. S-WAP is not defined. WSP (Wireless Session Protocol) and WDP (Wireless Datagram Protocol) are part of Wireless Access Protocol (WAP). Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 173).

QUESTION 141
What is the effective key size of DES?

A. 56 bits
B. 64 bits
C. 128 bits
D. 1024 bits

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Data Encryption Standard (DES) is a symmetric key algorithm. Originally developed by IBM, under project name Lucifer, this 128-bit algorithm was accepted by the NIST in 1974, but the total key size was reduced to 64 bits, 56 of which make up the effective key, plus and extra 8 bits for parity. It somehow became a national cryptographic standard in 1977, and an American National Standard Institute (ANSI) standard in 1978. DES was later replaced by the Advanced Encryption Standard (AES) by the NIST.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 8: Cryptography (page 525).

QUESTION 142
Which of the following offers confidentiality to an e-mail message?

A. The sender encrypting it with its private key.
B. The sender encrypting it with its public key.
C. The sender encrypting it with the receiver's public key.
D. The sender encrypting it with the receiver's private key.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: An e-mail message's confidentiality is protected when encrypted with the receiver's public key, because he is the only one able to decrypt the message. The sender is not supposed to have the receiver's private key. By encrypting a message with its private key, anybody possessing the corresponding public key would be able to read the message. By encrypting the message with its public key, not even the receiver would be able to read the message. Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 8: Cryptography (page 517).

QUESTION 143
Which of the following is not a DES mode of operation?

A. Cipher block chaining
B. Electronic code book
C. Input feedback
D. Cipher feedback

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Output feedback (OFB) is a DES mode of operation, not input feedback. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 149).

QUESTION 144
What size is an MD5 message digest (hash)?

A. 128 bits
B. 160 bits
C. 256 bits
D. 128 bytes

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: MD5 is a one-way hash function producing a 128-bit message digest from the input message, through 4 rounds of transformation. MD5 is specified as an Internet Standard (RFC1312).
Reference(s) used for this question:
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 145
Which of the following service is not provided by a public key infrastructure (PKI)?

A. Access control
B. Integrity
C. Authentication
D. Reliability

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: A Public Key Infrastructure (PKI) provides confidentiality, access control, integrity, authentication and non-repudiation.
It does not provide reliability services.
Reference(s) used for this question:
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 146
In a Public Key Infrastructure, how are public keys published?

A. They are sent via e-mail.
B. Through digital certificates.
C. They are sent by owners.
D. They are not published.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Public keys are published through digital certificates, signed by certification authority (CA), binding the certificate to the identity of its bearer.
A bit more details:
Although "Digital Certificates" is the best (or least wrong!) in the list of answers presented, for the past decade public keys have been published (ie: made known to the World) by the means of a LDAP server or a key distribution server (ex.: http://pgp.mit.edu/). An indirect publishing method is through OCSP servers (to validate digital signatures' CRL) Reference used for this question:
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.
and
http://technet.microsoft.com/en-us/library/dd361898.aspx

QUESTION 147
What principle focuses on the uniqueness of separate objects that must be joined together to perform a task? It is sometimes referred to as "what each must bring" and joined together when getting access or decrypting a file. Each of which does not reveal the other?

A. Dual control
B. Separation of duties
C. Split knowledge
D. Need to know

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Split knowledge involves encryption keys being separated into two components, each of which does not reveal the other. Split knowledge is the other complementary access control principle to dual control. In cryptographic terms, one could say dual control and split knowledge are properly implemented if no one person has access to or knowledge of the content of the complete cryptographic key being protected by the two rocesses.
The sound implementation of dual control and split knowledge in a cryptographic environment necessarily means that the quickest way to break the key would be through the best attack known for the algorithm of that key. The principles of dual control and split knowledge primarily apply to access to plaintext keys.
Access to cryptographic keys used for encrypting and decrypting data or access to keys that are encrypted under a master key (which may or may not be maintained under dual control and split knowledge) do not require dual control and split knowledge. Dual control and split knowledge can be summed up as the determination of any part of a key being protected must require the collusion between two or more persons with each supplying unique cryptographic materials that must be joined together to access the protected key. Any feasible method to violate the axiom means that the principles of dual control and split knowledge are not being upheld.
Split knowledge is the unique "what each must bring" and joined together when implementing dual control. To illustrate, a box containing petty cash is secured by one combination lock and one keyed lock. One employee is given the combination to the combo lock and another employee has possession of the correct key to the keyed lock.
In order to get the cash out of the box both employees must be present at the cash box at the same time. One cannot open the box without the other. This is the aspect of dual control. On the other hand, split knowledge is exemplified here by the different objects (the combination to the combo lock and the correct physical key), both of which are unique and necessary, that each brings to the meeting. Split knowledge focuses on the uniqueness of separate objects that must be joined together.
Dual control has to do with forcing the collusion of at least two or more persons to combine their split knowledge to gain access to an asset. Both split knowledge and dual control complement each other and are necessary functions that implement the segregation of duties in high integrity cryptographic environments.
The following are incorrect answers:
Dual control is a procedure that uses two or more entities (usually persons) operating in concert to protect a system resource, such that no single entity acting alone can access that resource. Dual control is implemented as a security procedure that requires two or more persons to come together and collude to complete a process. In a cryptographic system the two (or more) persons would each supply a unique key, that when taken together, performs a cryptographic process. Split knowledge is the other complementary access control principle to dual control. Separation of duties - The practice of dividing the steps in a system function among different individuals, so as to keep a single individual from subverting the process. The need-to-know principle requires a user having necessity for access to, knowledge of, or possession of specific information required to perform official tasks or services.
Reference(s) used for this question:
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition :
Cryptography (Kindle Locations 1621-1635). . Kindle Edition.
and
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition :
Cryptography (Kindle Locations 1643-1650). . Kindle Edition.
and
Shon Harris, CISSP All In One (AIO), 6th Edition , page 126

QUESTION 148
What level of assurance for a digital certificate verifies a user's name, address, social security number, and other information against a credit bureau database?

A. Level 1/Class 1
B. Level 2/Class 2
C. Level 3/Class 3

D. Level 4/Class 4

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Users can obtain certificates with various levels of assurance. Here is a list that describe each of them:
- Class 1/Level 1 for individuals, intended for email, no proof of identity For example, level 1 certificates verify electronic mail addresses. This is done through the use of a personal information number that a user would supply when asked to register. This level of certificate may also provide a name as well as an electronic mail address; however, it may or may not be a genuine name (i.e., it could be an alias). This proves that a human being will reply back if you send an email to that name or email address.
- Class 2/Level 2 is for organizations and companies for which proof of identity is required Level 2 certificates verify a user's name, address, social security number, and other information against a credit bureau database.
- Class 3/Level 3 is for servers and software signing, for which independent verification and checking of identity and authority is done by the issuing certificate authority Level 3 certificates are available to companies. This level of certificate provides photo identification to accompany the other items of information provided by a level 2 certificate.
- Class 4 for online business transactions between companies
- Class 5 for private organizations or governmental security

http://en.wikipedia.org/wiki/Digital_certificate veriSign introduced the concept of classes of digital certificates:
Also see:
Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 3, Secured Connections to External Networks (page 54).

QUESTION 149
Which of the following statements pertaining to stream ciphers is correct?

A. A stream cipher is a type of asymmetric encryption algorithm.
B. A stream cipher generates what is called a keystream.
C. A stream cipher is slower than a block cipher.
D. A stream cipher is not appropriate for hardware-based encryption.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: A stream cipher is a type of symmetric encryption algorithm that operates on continuous streams of plain text and is appropriate for hardware-based encryption. Stream ciphers can be designed to be exceptionally fast, much faster than any block cipher. A stream cipher generates what is called a keystream (a sequence of bits used as a key). Stream ciphers can be viewed as approximating the action of a proven unbreakable cipher, the one-time pad (OTP), sometimes known as the Vernam cipher. A one-time pad uses a keystream of completely random digits. The keystream is combined with the plaintext digits one at a time to form the ciphertext. This system was proved to be secure by Claude Shannon in 1949. However, the keystream must be (at least) the same length as the plaintext, and generated completely at random. This makes the system very cumbersome to implement in practice, and as a result the one-time pad has not been widely used, except for the most critical applications. A stream cipher makes use of a much smaller and more convenient key -- 128 bits, for example. Based on this key, it generates a pseudorandom keystream which can be combined with the plaintext digits in a similar fashion to the one-time pad. However, this comes at a cost: because the keystream is now pseudorandom, and not truly random, the proof of security associated with the one-time pad no longer holds: it is quite possible for a stream cipher to be completely insecure if it is not implemented properly as we have seen with the Wired Equivalent Privacy (WEP) protocol.
Encryption is accomplished by combining the keystream with the plaintext, usually with the bitwise XOR operation.
Source: DUPUIS, Clement, CISSP Open Study Guide on domain 5, cryptography, April 1999. More details can be obtained on Stream Ciphers in RSA Security's FAQ on Stream Ciphers.

QUESTION 150
Which of the following statements pertaining to block ciphers is incorrect?

A. It operates on fixed-size blocks of plaintext.
B. It is more suitable for software than hardware implementations.
C. Plain text is encrypted with a public key and decrypted with a private key.
D. Some Block ciphers can operate internally as a stream.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Block ciphers do not use public cryptography (private and public keys). Block ciphers is a type of symmetric-key encryption algorithm that transforms a fixed-size block of plaintext (unencrypted text) data into a block of ciphertext (encrypted text) data of the same length. They are appropriate for software implementations and can operate internally as a stream. See more info below about DES in Output Feedback Mode (OFB), which makes use internally of a stream cipher.
The output feedback (OFB) mode makes a block cipher into a synchronous stream cipher. It generates keystream blocks, which are then XORed with the plaintext blocks to get the ciphertext. Just as with other stream ciphers, flipping a bit in the ciphertext produces a flipped bit in the plaintext at the same location. This property allows many error correcting codes to function normally even when applied before encryption.
Reference(s) used for this question:
Wikipedia on Block Cipher mode at: https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation and http://www.itl.nist.gov/fipspubs/fip81.htm

QUESTION 151
Cryptography does NOT help in:

A. Detecting fraudulent insertion.
B. Detecting fraudulent deletion.
C. Detecting fraudulent modification.
D. Detecting fraudulent disclosure.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Cryptography is a detective control in the fact that it allows the detection of fraudulent insertion, deletion or modification. It also is a preventive control is the fact that it prevents disclosure, but it usually does not offers any means of detecting disclosure. Source: DUPUIS, Clement, CISSP Open Study Guide on domain 5, cryptography, April 1999.

QUESTION 152
What is used to bind a document to its creation at a particular time?

A. Network Time Protocol (NTP)
B. Digital Signature
C. Digital Timestamp
D. Certification Authority (CA)

Correct Answer: C
Explanation

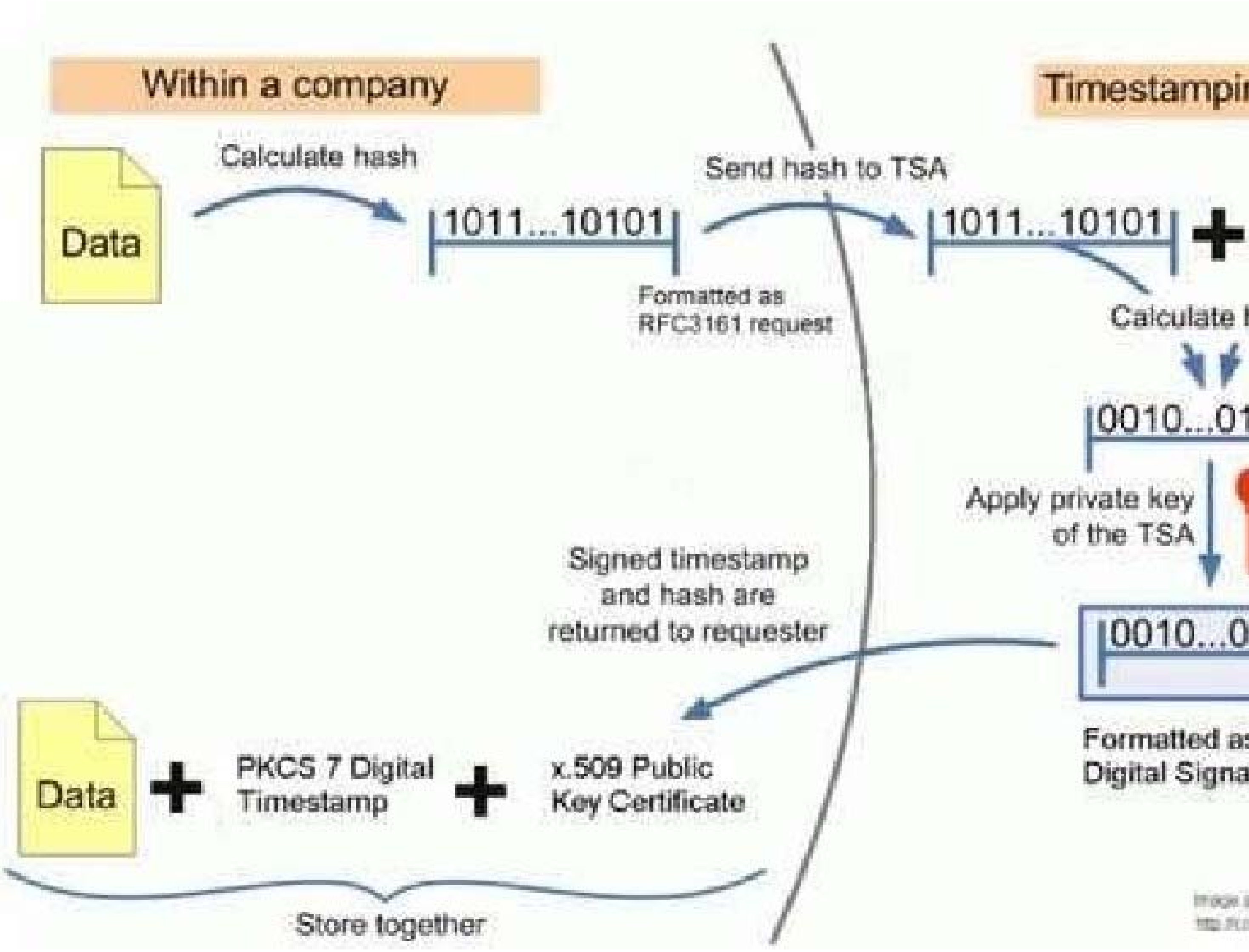
Explanation/Reference:
Explanation: While a digital signature binds a document to the possessor of a particular key, a digital

timestamp binds a document to its creation at a particular time. Trusted timestamping is the process of securely keeping track of the creation and modification time of a document. Security here means that no one -- not even the owner of the document -- should be able to change it once it has been recorded provided that the timestamper's integrity is never compromised.

The administrative aspect involves setting up a publicly available, trusted timestamp management infrastructure to collect, process and renew timestamps or to make use of a commercially available time stamping service.

A modern example of using a Digital Timestamp is the case of an industrial research organization that may later need to prove, for patent purposes, that they made a particular discovery on a particular date; since magnetic media can be altered easily, this may be a nontrivial issue. One possible solution is for a researcher to compute and record in a hardcopy laboratory notebook a cryptographic hash of the relevant data file. In the future, should there be a need to prove the version of this file retrieved from a backup tape has not been altered, the hash function could be recomputed and compared with the hash value recorded in that paper notebook. According to the RFC 3161 standard, a trusted timestamp is a timestamp issued by a trusted third party (TTP) acting as a Time Stamping Authority (TSA). It is used to prove the existence of certain data before a certain point (e.g. contracts, research data, medical records,...) without the possibility that the owner can backdate the timestamps. Multiple TSAs can be used to increase reliability and reduce vulnerability.

The newer ANSI ASC X9.95 Standard for trusted timestamps augments the RFC 3161 standard with data-level security requirements to ensure data integrity against a reliable time source that is provable to any third party. This standard has been applied to authenticating digitally signed data for regulatory compliance, financial transactions, and legal evidence.



Digital TimeStamp
The following are incorrect answers:
Network Time Protocol (NTP) is used to achieve high accuracy time synchronization for computers across a network.
A Certification Authority (CA) is the entity responsible for the issuance of digital certificates. A Digital Signature provides integrity and authentication but does not bind a document to a specific time it was created.
Reference used for this question:
http://en.m.wikipedia.org/wiki/File:Trusted_timestamping.gif and
http://en.wikipedia.org/wiki/Trusted_timestamping

QUESTION 153
Which of the following is best at defeating frequency analysis?

A. Substitution cipher
B. Polyalphabetic cipher
C. Transposition cipher
D. Ceasar Cipher

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Simple substitution and transposition ciphers are vulnerable to attacks that perform frequency analysis.
In every language, there are words and patterns that are used more than others. Some patterns common to a language can actually help attackers figure out the transformation between plaintext and ciphertext, which enables them to figure out the key that was used to perform the transformation. Polyalphabetic ciphers use different alphabets to defeat frequency analysis.
The ceasar cipher is a very simple substitution cipher that can be easily defeated and it does show repeating letters.
Out of list presented, it is the Polyalphabetic cipher that would provide the best protection against simple frequency analysis attacks.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 8: Cryptography (page 507).
And : DUPUIS, Clement, CISSP Open Study Guide on domain 5, cryptography, April 1999.

QUESTION 154
A code, as is pertains to cryptography:

A. Is a generic term for encryption.
B. Is specific to substitution ciphers.
C. Deals with linguistic units.
D. Is specific to transposition ciphers.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Historically, a code refers to a cryptosystem that deals with linguistic units: words, phrases, sentences, and so forth. Codes are only useful for specialized circumstances where the message to transmit has an already defined equivalent ciphertext word. Source: DUPUIS, Cl?ment, CISSP Open Study Guide on domain 5, cryptography, April 1999.

QUESTION 155
Which of the following is the most secure form of triple-DES encryption?

A. DES-EDE3
B. DES-EDE1
C. DES-EEE4
D. DES-EDE2

Correct Answer: A
Explanation

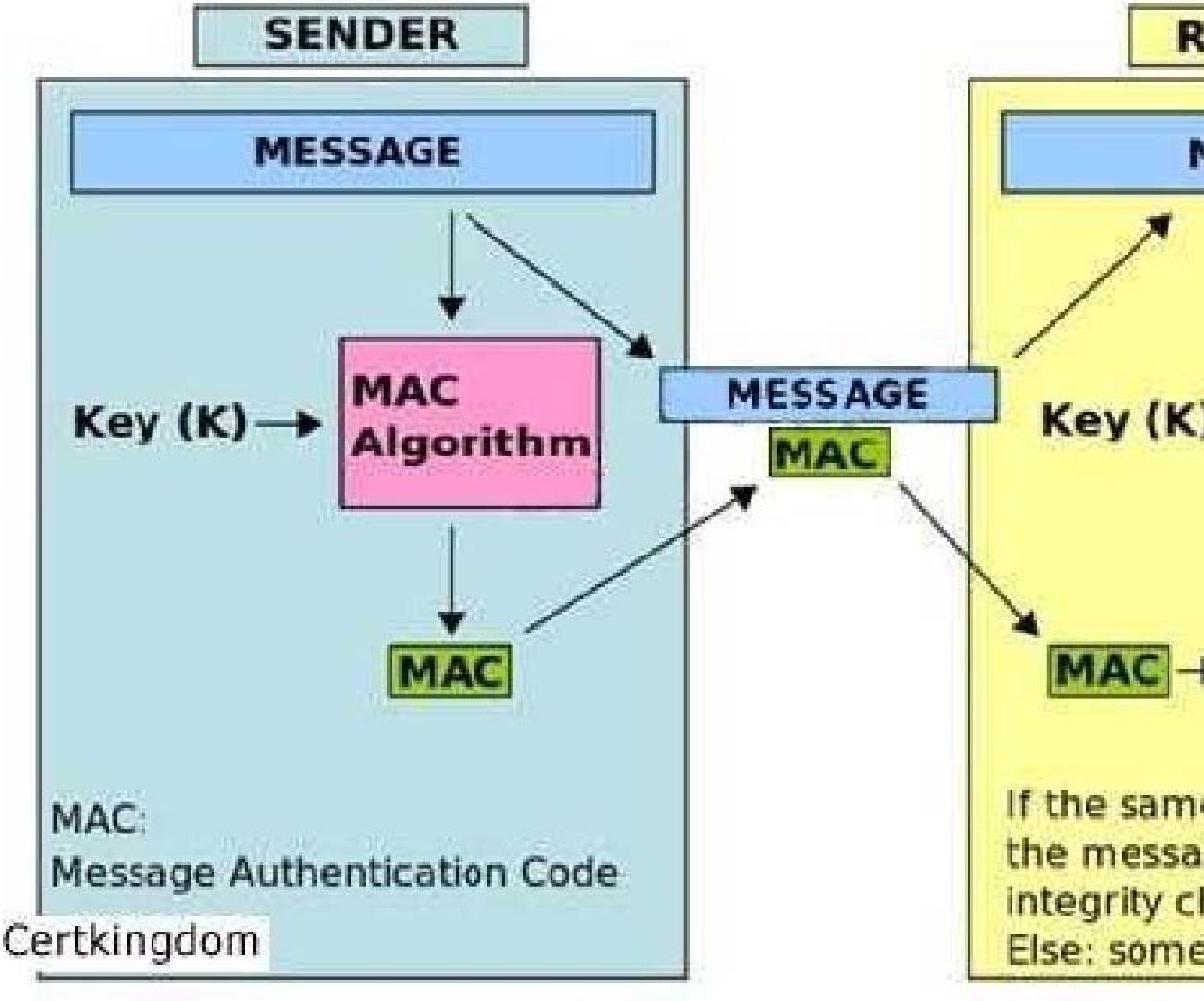
Explanation/Reference:
Explanation: Triple DES with three distinct keys is the most secure form of triple-DES encryption. It can either be DES-EEE3 (encrypt-encrypt-encrypt) or DES-EDE3 (encrypt-decrypt-encrypt). DES-EDE1 is not defined and would mean using a single key to encrypt, decrypt and encrypt again, equivalent to single DES. DES-EEE4 is not defined and DES-EDE2 uses only 2 keys (encrypt with first key, decrypt with second key, encrypt with first key again). Source: DUPUIS, Cl?ment, CISSP Open Study Guide on domain 5, cryptography, April 1999.

QUESTION 156
Which of the following is NOT a known type of Message Authentication Code (MAC)?

A. Keyed-hash message authentication code (HMAC)
B. DES-CBC
C. Signature-based MAC (SMAC)
D. Universal Hashing Based MAC (UMAC)

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: There is no such thing as a Signature-Based MAC. Being the wrong choice in the list, it is the best answer to this question.
WHAT IS A Message Authentication Code (MAC)?
In Cryptography, a MAC (Message Authentication Code) also known as a cryptographic checksum, is a small block of data that is generated using a secret key and then appended to the message. When the message is received, the recipient can generate their own MAC using the secret key, and thereby know that the message has not changed either accidentally or intentionally in transit. Of course, this assurance is only as strong as the trust that the two parties have that no one else has access to the secret key.
A MAC is a small representation of a message and has the following characteristics:
A MAC is much smaller than the message generating it.
Given a MAC, it is impractical to compute the message that generated it. Given a MAC and the message that generated it, it is impractical to find another message generating the same MAC.
See the graphic below from Wikipedia showing the creation of a MAC value:



Message Authentication Code MAC HMAC
In the example above, the sender of a message runs it through a MAC algorithm to produce a MAC data tag. The message and the MAC tag are then sent to the receiver. The receiver in turn runs the message portion of the transmission through the same MAC algorithm using the same key, producing a second MAC data tag. The receiver then compares the first MAC tag received in the transmission to the second generated MAC tag. If they are identical, the receiver can safely assume that the integrity of the message was not compromised, and the message was not altered or tampered with during transmission.
However, to allow the receiver to be able to detect replay attacks, the message itself must contain data that assures that this same message can only be sent once (e.g. time stamp, sequence number or use of a one-time MAC). Otherwise an attacker could -- without even understanding its content -- record this message and play it back at a later time, producing the same result as the original sender.
NOTE: There are many ways of producing a MAC value. Below you have a short list of some implementation.
The following were incorrect answers for this question:
They were all incorrect answers because they are all real type of MAC implementation. In the case of DES-CBC, a MAC is generated using the DES algorithm in CBC mode, and the secret DES key is shared by the sender and the receiver. The MAC is actually just the last block of ciphertext generated by the algorithm. This block of data (64 bits) is attached to the unencrypted message and transmitted to the far end. All previous

blocks of encrypted data are discarded to prevent any attack on the MAC itself. The receiver can just generate his own MAC using the secret DES key he shares to ensure message integrity and authentication. He knows that the message has not changed because the chaining function of CBC would significantly alter the last block of data if any bit had changed anywhere in the message. He knows the source of the message (authentication) because only one other person holds the secret key. A Keyed-hash message authentication code (HMAC) is a specific construction for calculating a message authentication code (MAC) involving a cryptographic hash function in combination with a secret cryptographic key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authentication of a message. Any cryptographic hash function, such as MD5, SHA-1, may be used in the calculation of an HMAC; the resulting MAC algorithm is termed HMACMD5 or HMAC-SHA1 accordingly. The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, the size of its hash output, and on the size and quality of the key.
A message authentication code based on universal hashing, or UMAC, is a type of message authentication code (MAC) calculated choosing a hash function from a class of hash functions according to some secret (random) process and applying it to the message. The resulting digest or fingerprint is then encrypted to hide the identity of the hash function used. As with any MAC, it may be used to simultaneously verify both the data integrity and the authenticity of a message. UMAC is specified in RFC 4418, it has provable cryptographic strength and is usually a lot less computationally intensive than other MACs.
What is the MicMac (confusion) with MIC and MAC?
The term message integrity code (MIC) is frequently substituted for the term MAC, especially in communications, where the acronym MAC traditionally stands for Media Access Control when referring to Networking. However, some authors use MIC as a distinctly different term from a MAC; in their usage of the term the MIC operation does not use secret keys. This lack of security means that any MIC intended for use gauging message integrity should be encrypted or otherwise be protected against tampering. MIC algorithms are created such that a given message will always produce the same MIC assuming the same algorithm is used to generate both. Conversely, MAC algorithms are designed to produce matching MACs only if the same message, secret key and initialization vector are input to the same algorithm. MICs do not use secret keys and, when taken on their own, are therefore a much less reliable gauge of message integrity than MACs. Because MACs use secret keys, they do not necessarily need to be encrypted to provide the same level of assurance.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 15799-15815). Auerbach Publications. Kindle Edition.
and
http://en.wikipedia.org/wiki/Message_authentication_code and
http://tools.ietf.org/html/rfc4418

QUESTION 157
What is the maximum key size for the RC5 algorithm?

A. 128 bits
B. 256 bits
C. 1024 bits
D. 2040 bits

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: RC5 is a fast block cipher created by Ron Rivest and analyzed by RSA Data Security, Inc.
It is a parameterized algorithm with a variable block size, a variable key size, and a variable number of rounds. Allowable choices for the block size are 32 bits (for experimentation and evaluation purposes only), 64 bits (for use a drop-in replacement for DES), and 128 bits. The number of rounds can range from 0 to 255, while the key can range from 0 bits to 2040 bits in size.
Please note that some sources such as the latest Shon Harris book mentions that RC5 maximum key size is of 2048, not 2040 bits. I would definitively use RSA as the authoritative source which specifies a key of 2040 bits. It is an error in Shon's book.
The OIG book says:
RC5 was developed by Ron Rivest of RSA and is deployed in many of RSA's products. It is a very adaptable product useful for many applications, ranging from software to hardware implementations. The key for RC5

can vary from 0 to 2040 bits, the number of rounds it executes can be adjusted from 0 to 255, and the length of the input words can also be chosen from 16-, 32-, and 64-bit lengths.
The following answers were incorrect choices:
All of the other answers were wrong.
Reference(s) used for this question:
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition :
Cryptography (Kindle Locations 1098-1101). . Kindle Edition. Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 16744- 16747). McGraw-Hill. Kindle Edition.
http://www.rsa.com/rsalabs/node.asp?id=2251, What are RC5 and RC6, RSA The Security Division of EMC.
From Rivest himself, see http://people.csail.mit.edu/rivest/Rivest-rc5rev.pdf Also see the draft IETF IPSEC standard which clearly mention that it is in fact 2040 bits as a MAXIMUM key size:
http://www.tools.ietf.org/html/draft-ietf-ipsec-esp-rc5-cbc-00 http://en.wikipedia.org/wiki/RC5, Mention a maximum key size of 2040 as well.

QUESTION 158
Which of the following algorithms is a stream cipher?

A. RC2
B. RC4
C. RC5
D. RC6

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: RC2, RC4, RC5 and RC6 were developed by Ronal Rivest from RSA Security.
In the RC family only RC4 is a stream cipher.
RC4 allows a variable key length.
RC2 works with 64-bit blocks and variable key lengths, RC5 has variable block sizes, key length and number of processing rounds.
RC6 was designed to fix a flaw in RC5.
Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 6: Cryptography (page 103).

QUESTION 159
In a SSL session between a client and a server, who is responsible for generating the master secret that will be used as a seed to generate the symmetric keys that will be used during the session?

A. Both client and server
B. The client's browser
C. The web server
D. The merchant's Certificate Server

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Once the merchant server has been authenticated by the browser client, the browser generates a master secret that is to be shared only between the server and client. This secret serves as a seed to generate the session (private) keys. The master secret is then encrypted with the merchant's public key and sent to the server. The fact that the master secret is generated by the client's browser provides the client assurance that the server is not reusing keys that would have been used in a previous session with another client. Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 6: Cryptography (page 112).
Also: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, page 569.

QUESTION 160
Which of the following is less likely to be used today in creating a Virtual Private Network?

A. L2TP
B. PPTP
C. IPSec
D. L2F

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: L2F (Layer 2 Forwarding) provides no authentication or encryption. It is a Protocol that supports the creation of secure virtual private dial-up networks over the Internet. At one point L2F was merged with PPTP to produce L2TP to be used on networks and not only on dial up links.
IPSec is now considered the best VPN solution for IP environments. Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 8: Cryptography (page 507).

QUESTION 161
Which of the following was not designed to be a proprietary encryption algorithm?

A. RC2
B. RC4
C. Blowfish
D. Skipjack

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Blowfish is a symmetric block cipher with variable-length key (32 to 448 bits) designed in 1993 by Bruce Schneier as an unpatented, license-free, royalty-free replacement for DES or IDE
A. See attributes below:
Block cipher: 64-bit block
Variable key length: 32 bits to 448 bits
Designed by Bruce Schneier
Much faster than DES and IDEA
Unpatented and royalty-free
No license required
Free source code available
Rivest Cipher #2 (RC2) is a proprietary, variable-key-length block cipher invented by Ron Rivest for RSA Data Security, Inc.
Rivest Cipher #4 (RC4) is a proprietary, variable-key-length stream cipher invented by Ron Rivest for RSA Data Security, Inc.
The Skipjack algorithm is a Type II block cipher [NIST] with a block size of 64 bits and a key size of 80 bits that was developed by NSA and formerly classified at the U.S. Department of Defense "Secret" level. The NSA announced on June 23, 1998, that Skipjack had been declassified.
RSA Laboratories
http://www.rsa.com/rsalabs/node.asp?id=2250
RFC 2828 - Internet Security Glossary
http://www.faqs.org/rfcs/rfc2828.html

QUESTION 162
Which of the following is not an encryption algorithm?

A. Skipjack
B. SHA-1
C. Twofish

D. DEA

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The SHA-1 is a hashing algorithm producing a 160-bit hash result from any data. It does not perform encryption.
In cryptography, SHA-1 is a cryptographic hash function designed by the United States National Security Agency and published by the United States NIST as a U.S. Federal Information Processing Standard.
SHA stands for "secure hash algorithm". The four SHA algorithms are structured differently and are distinguished as SHA-0, SHA-1, SHA-2, and SHA-3. SHA-1 is very similar to SHA-0, but corrects an error in the original SHA hash specification that led to significant weaknesses. The SHA-0 algorithm was not adopted by many applications. SHA-2 on the other hand significantly differs from the SHA-1 hash function.
SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used applications and protocols.
In 2005, cryptanalysts found attacks on SHA-1 suggesting that the algorithm might not be secure enough for ongoing use. NIST required many applications in federal agencies to move to SHA-2 after 2010 because of the weakness. Although no successful attacks have yet been reported on SHA-2, they are algorithmically similar to SHA-1.
In 2012, following a long-running competition, NIST selected an additional algorithm, Keccak, for standardization as SHA-3
NOTE:
A Cryptographic Hash Function is not the same as an Encryption Algorithm even thou both are Algorithms. An algorithm is defined as a step-by-step procedure for calculations. Hashing Algorithm do not encrypt the data. People sometimes will say they encrypted a password with SHA-1 but really they simply created a Message Digest of the password using SHA-1, putting the input through a series of steps to come out with the message digest or hash value. A cryptographic hash function is a hash function; that is, an algorithm that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that any (accidental or intentional) change to the data will (with very high probability) change the hash value. The data to be encoded are often called the "message," and the hash value is sometimes called the message digest or simply digest.
Encryption Algorithms are reversible but Hashing Algorithms are not meant to be reversible if the input is large enough.
The following are incorrect answers:
The Skipjack algorithm is a Type II block cipher with a block size of 64 bits and a key size of 80 bits that was developed by NSA and formerly classified at the U.S. Department of Defense "Secret" level.
Twofish is a freely available 128-bit block cipher designed by Counterpane Systems (Bruce Schneier et al.).
DEA is a symmetric block cipher, defined as part of the U.S. Government's Data Encryption Standard (DES). DEA uses a 64-bit key, of which 56 bits are independently chosen and 8 are parity bits, and maps a 64-bit block into another 64-bit block.
Reference(s) used for this question:
http://en.wikipedia.org/wiki/SHA-1
and
SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.
and
Counterpane Labs, at http://www.counterpane.com/twofish.html.

QUESTION 163
What key size is used by the Clipper Chip?

A. 40 bits
B. 56 bits
C. 64 bits
D. 80 bits

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The Clipper Chip is a NSA designed tamperproof chip for encrypting data and it uses the SkipJack algorithm. Each Clipper Chip has a unique serial number and a copy of the unit key is stored in the database under this serial number. The sending Clipper Chip generates and sends a Law Enforcement Access Field (LEAF) value included in the transmitted message. It is based on a 80-bit key and a 16-bit checksum.
Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 1).

QUESTION 164
Which of the following would best describe a Concealment cipher?

A. Permutation is used, meaning that letters are scrambled.
B. Every X number of words within a text, is a part of the real message.
C. Replaces bits, characters, or blocks of characters with different bits, characters or blocks.
D. Hiding data in another message so that the very existence of the data is concealed.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: When a concealment cipher is used, every X number of words within a text, is a part of the real message. The message is within another message. A concealment cipher is a message within a message. If my other super-secret spy buddy and I decide our key value is every third word, then when I get a message from him, I will pick out every third word and write it down. Suppose he sends me a message that reads, "The saying, `The time is right' is not cow language, so is now a dead subject." Because my key is every third word, I come up with "The right cow is dead." This again means nothing to me, and I am now turning in my decoder ring.
Concealment ciphers include the plaintext within the ciphertext. It is up to the recipient to know which letters or symbols to exclude from the ciphertext in order to yield the plaintext. Here is an example of a concealment cipher:
i2l32i5321k34e1245ch456oc12ol234at567e
Remove all the numbers, and you'll have i like chocolate. How about this one? Larry even appears very excited. No one worries.
The first letter from each word reveals the message leave now. Both are easy, indeed, but many people have crafted more ingenious ways of concealing the messages. By the way, this type of cipher doesn't even need ciphertext, such as that in the above examples. Consider the invisible drying ink that kids use to send secret messages. In a more extreme example, a man named Histiaeus, during 5th century B.C., shaved the head of a trusted slave, then tattooed the message onto his bald head. When the slave's hair grew back, Histiaeus sent the slave to the message's intended recipient, Aristagoros, who shaved the slave's head and read the message instructing him to revolt.
The following answers are incorrect:
A transposition cipher uses permutations.
A substitution cipher replaces bits, characters, or blocks of characters with different bits, characters or blocks.
Steganography refers to hiding the very existence of the message. Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 1).
and also see:
http://www.go4expert.com/forums/showthread.php?t=415

QUESTION 165
Which of the following is best provided by symmetric cryptography?

A. Confidentiality
B. Integrity
C. Availability
D. Non-repudiation

Correct Answer: A

Explanation

Explanation/Reference:
Explanation: When using symmetric cryptography, both parties will be using the same key for encryption and decryption. Symmetric cryptography is generally fast and can be hard to break, but it offers limited overall security in the fact that it can only provide confidentiality. Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 2).

QUESTION 166
Which of the following is not a disadvantage of symmetric cryptography when compared with Asymmetric Ciphers?

A. Provides Limited security services
B. Has no built in Key distribution
C. Speed
D. Large number of keys are needed

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Symmetric cryptography ciphers are generally fast and hard to break. So speed is one of the key advantage of Symmetric ciphers and NOT a disadvantage. Symmetric Ciphers uses simple encryption steps such as XOR, substitution, permutation, shifting columns, shifting rows, etc... Such steps does not required a large amount of processing power compare to the complex mathematical problem used within Asymmetric Ciphers.
Some of the weaknesses of Symmetric Ciphers are:
The lack of automated key distribution. Usually an Asymmetric cipher would be use to protect the symmetric key if it needs to be communicated to another entity securely over a public network. In the good old day this was done manually where it was distributed using the Floppy Net sometimes called the Sneaker Net (you run to someone's office to give them the key). As far as the total number of keys are required to communicate securely between a large group of users, it does not scale very well. 10 users would require 45 keys for them to communicate securely with each other. If you have 1000 users then you would need almost half a million key to communicate secure. On Asymmetric ciphers there is only 2000 keys required for 1000 users. The formula to calculate the total number of keys required for a group of users who wishes to communicate securely with each others using Symmetric encryption is Total Number of Users (N)
* Total Number of users minus one Divided by 2 or N (N-1)/2 Symmetric Ciphers are limited when it comes to security services, they cannot provide all of the security services provided by Asymmetric ciphers. Symmetric ciphers provides mostly confidentiality but can also provide integrity and authentication if a Message Authentication Code (MAC) is used and could also provide user authentication if Kerberos is used for example. Symmetric Ciphers cannot provide Digital Signature and Non-Repudiation.
Reference used for theis question:
WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 2).

QUESTION 167
Which of the following is more suitable for a hardware implementation?

A. Stream ciphers
B. Block ciphers
C. Cipher block chaining
D. Electronic code book

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: A stream cipher treats the message as a stream of bits or bytes and performs mathematical

functions on them individually. The key is a random value input into the stream cipher, which it uses to ensure the randomness of the keystream data. They are more suitable for hardware implementations, because they encrypt and decrypt one bit at a time. They are intensive because each bit must be manipulated, which works better at the silicon level. Block ciphers operate a the block level, dividing the message into blocks of bits. Cipher Block chaining (CBC) and Electronic Code Book (ECB) are operation modes of DES, a block encryption algorithm. Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 2).

QUESTION 168
How many rounds are used by DES?

A. 16
B. 32
C. 64
D. 48

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: DES is a block encryption algorithm using 56-bit keys and 64-bit blocks that are divided in half and each character is encrypted one at a time. The characters are put through 16 rounds of transposition and substitution functions. Triple DES uses 48 rounds. Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 3).

QUESTION 169
What is the key size of the International Data Encryption Algorithm (IDEA)?

A. 64 bits
B. 128 bits
C. 160 bits
D. 192 bits

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The International Data Encryption Algorithm (IDEA) is a block cipher that operates on 64 bit blocks of data with a 128-bit key. The data blocks are divided into 16 smaller blocks and each has eight rounds of mathematical functions performed on it. It is used in the PGP encryption software.
Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 3).

QUESTION 170
Which of the following is not an example of a block cipher?

A. Skipjack
B. IDEA
C. Blowfish
D. RC4

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: RC4 is a proprietary, variable-key-length stream cipher invented by Ron Rivest for RSA Data Security, Inc. Skipjack, IDEA and Blowfish are examples of block ciphers. Source: SHIREY, Robert W.,

RFC2828: Internet Security Glossary, may 2000.

QUESTION 171
The Diffie-Hellman algorithm is used for:

A. Encryption
B. Digital signature
C. Key agreement
D. Non-repudiation

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The Diffie-Hellman algorithm is used for Key agreement (key distribution) and cannot be used to encrypt and decrypt messages.
Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 4). Note: key agreement, is different from key exchange, the functionality used by the other asymmetric algorithms.
AIO, third edition Cryptography (Page 632)
AIO, fourth edition Cryptography (Page 709)

QUESTION 172
A one-way hash provides which of the following?

A. Confidentiality
B. Availability
C. Integrity
D. Authentication

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: A one-way hash is a function that takes a variable-length string a message, and compresses and transforms it into a fixed length value referred to as a hash value. It provides integrity, but no confidentiality, availability or authentication. Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 5).

QUESTION 173
Which of the following is not a one-way hashing algorithm?

A. MD2
B. RC4
C. SHA-1
D. HAVAL

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: RC4 was designed by Ron Rivest of RSA Security in 1987. While it is officially termed "Rivest Cipher 4", the RC acronym is alternatively understood to stand for "Ron's Code" (see also RC2, RC5 and RC6).
RC4 was initially a trade secret, but in September 1994 a description of it was anonymously posted to the Cypherpunks mailing list. It was soon posted on the sci.crypt newsgroup, and from there to many sites on the Internet. The leaked code was confirmed to be genuine as its output was found to match that of proprietary

software using licensed RC4. Because the algorithm is known, it is no longer a trade secret. The name RC4 is trademarked, so RC4 is often referred to as ARCFOUR or ARC4 (meaning alleged RC4) to avoid trademark problems. RSA Security has never officially released the algorithm; Rivest has, however, linked to the English Wikipedia article on RC4 in his own course notes. RC4 has become part of some commonly used encryption protocols and standards, including WEP and WPA for wireless cards and TLS. The main factors in RC4's success over such a wide range of applications are its speed and simplicity: efficient implementations in both software and hardware are very easy to develop.
The following answer were not correct choices:
SHA-1 is a one-way hashing algorithms. SHA-1 is a cryptographic hash function designed by the United States National Security Agency and published by the United States NIST as a U.S. Federal Information Processing Standard. SHA stands for "secure hash algorithm". The three SHA algorithms are structured differently and are distinguished as SHA-0, SHA-1, and SHA-2. SHA-1 is very similar to SHA-0, but corrects an error in the original SHA hash specification that led to significant weaknesses. The SHA-0 algorithm was not adopted by many applications. SHA-2 on the other hand significantly differs from the SHA-1 hash function. SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used security applications and protocols. In 2005, security flaws were identified in SHA-1, namely that a mathematical weakness might exist, indicating that a stronger hash function would be desirable. Although no successful attacks have yet been reported on the SHA-2 variants, they are algorithmically similar to SHA-1 and so efforts are underway to develop improved alternatives. A new hash standard, SHA-3, is currently under development -- an ongoing NIST hash function competition is scheduled to end with the selection of a winning function in 2012. SHA-1 produces a 160-bit message digest based on principles similar to those used by Ronald L. Rivest of MIT in the design of the MD4 and MD5 message digest algorithms, but has a more conservative design.
MD2 is a one-way hashing algorithms. The MD2 Message-Digest Algorithm is a cryptographic hash function developed by Ronald Rivest in 1989. The algorithm is optimized for 8-bit computers. MD2 is specified in RFC 1319. Although MD2 is no longer considered secure, even as of 2010 it remains in use in public key infrastructures as part of certificates generated with MD2 and RSA. Haval is a one-way hashing algorithms. HAVAL is a cryptographic hash function. Unlike MD5, but like most modern cryptographic hash functions, HAVAL can produce hashes of different lengths. HAVAL can produce hashes in lengths of 128 bits, 160 bits, 192 bits, 224 bits, and 256 bits. HAVAL also allows users to specify the number of rounds (3, 4, or 5) to be used to generate the hash.
The following reference(s) were used for this question:
SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.
and
https://en.wikipedia.org/wiki/HAVAL
and
https://en.wikipedia.org/wiki/MD2_%28cryptography%29
and
https://en.wikipedia.org/wiki/SHA-1

QUESTION 174
Which of the following statements pertaining to key management is incorrect?

A. The more a key is used, the shorter its lifetime should be.
B. When not using the full keyspace, the key should be extremely random.
C. Keys should be backed up or escrowed in case of emergencies.
D. A key's lifetime should correspond with the sensitivity of the data it is protecting.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: A key should always be using the full spectrum of the keyspace and be extremely random. Other statements are correct.
Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 6).

QUESTION 175
Which of the following statements pertaining to link encryption is false?

A. It encrypts all the data along a specific communication path.
B. It provides protection against packet sniffers and eavesdroppers.
C. Information stays encrypted from one end of its journey to the other.
D. User information, header, trailers, addresses and routing data that are part of the packets are encrypted.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: When using link encryption, packets have to be decrypted at each hop and encrypted again.
Information staying encrypted from one end of its journey to the other is a characteristic of end-toend encryption, not link encryption.
Link Encryption vs. End-to-End Encryption
Link encryption encrypts the entire packet, including headers and trailers, and has to be decrypted at each hop.
End-to-end encryption does not encrypt the IP Protocol headers, and therefore does not need to be decrypted at each hop.
All in one, Page 735 & Glossary
and
Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 6).

QUESTION 176
Cryptography does not concern itself with which of the following choices?

A. Availability
B. Integrity
C. Confidentiality
D. Validation

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The cryptography domain addresses the principles, means, and methods of disguising information to ensure its integrity, confidentiality, and authenticity. Unlike the other domains, cryptography does not completely support the standard of availability.
Availability
Cryptography supports all three of the core principles of information security. Many access control systems use cryptography to limit access to systems through the use of passwords. Many tokenbased authentication systems use cryptographic-based hash algorithms to compute one-time passwords. Denying unauthorized access prevents an attacker from entering and damaging the system or network, thereby denying access to authorized users if they damage or currupt the data.
Confidentiality
Cryptography provides confidentiality through altering or hiding a message so that ideally it cannot be understood by anyone except the intended recipient.
Integrity
Cryptographic tools provide integrity checks that allow a recipient to verify that a message has not been altered. Cryptographic tools cannot prevent a message from being altered, but they are effective to detect either intentional or accidental modification of the message. Additional Features of Cryptographic Systems In addition to the three core principles of information security listed above, cryptographic tools provide several more benefits.
Nonrepudiation
In a trusted environment, the authentication of the origin can be provided through the simple control of the keys. The receiver has a level of assurance that the message was encrypted by the sender, and the sender has trust that the message was not altered once it was received. However, in a more stringent, less trustworthy environment, it may be necessary to provide assurance via a third party of who sent a message and that the message was indeed delivered to the right recipient. This is accomplished through the use of digital signatures

and public key encryption. The use of these tools provides a level of nonrepudiation of origin that can be verified by a third party. Once a message has been received, what is to prevent the recipient from changing the message and contesting that the altered message was the one sent by the sender? The nonrepudiation of delivery prevents a recipient from changing the message and falsely claiming that the message is in its original state. This is also accomplished through the use of public key cryptography and digital signatures and is verifiable by a trusted third party.

Authentication

Authentication is the ability to determine if someone or something is what it declares to be. This is primarily done through the control of the keys, because only those with access to the key are able to encrypt a message. This is not as strong as the nonrepudiation of origin, which will be reviewed shortly Cryptographic functions use several methods to ensure that a message has not been changed or altered. These include hash functions, digital signatures, and message authentication codes (MACs). The main concept is that the recipient is able to detect any change that has been made to a message, whether accidentally or intentionally.

Access Control

Through the use of cryptographic tools, many forms of access control are supported--from log-ins via passwords and passphrases to the prevention of access to confidential files or messages. In all cases, access would only be possible for those individuals that had access to the correct cryptographic keys.

NOTE FROM CLEMENT:

As you have seen this question was very recently updated with the latest content of the Official ISC2 Guide (OIG) to the CISSP CBK, Version 3.

Myself, I agree with most of you that cryptography does not help on the availability side and it is even the contrary sometimes if you loose the key for example. In such case you would loose access to the data and negatively impact availability. But the ISC2 is not about what I think or what you think, they have their own view of the world where they claim and state clearly that cryptography does address availability even thou it does not fully address it. They look at crypto as the ever emcompassing tool it has become today. Where it can be use for authentication purpose for example where it would help to avoid corruption of the data through illegal access by an unauthorized user.

The question is worded this way in purpose, it is VERY specific to the CISSP exam context where ISC2 preaches that cryptography address availability even thou they state it does not fully address it. This is something new in the last edition of their book and something you must be aware of.

Best regards

Clement

The following terms are from the Software Development Security domain:

Validation: The assurance that a product, service, or system meets the needs of the customer and other identified stakeholders. It often involves acceptance and suitability with external customers.

Contrast with verification below."

Verification: The evaluation of whether or not a product, service, or system complies with a regulation, requirement, specification, or imposed condition. It is often an internal process.

Contrast with validation."

The terms above are from the Software Development Security Domain.

Reference(s) used for this question:

Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Cryptography (Kindle Locations 227-244). . Kindle Edition.

and

Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Cryptography (Kindle Locations 206-227). . Kindle Edition.

and

http://en.wikipedia.org/wiki/Verification_and_validation

QUESTION 177

Which of the following does NOT concern itself with key management?

A. Internet Security Association Key Management Protocol (ISAKMP)

B. Diffie-Hellman (DH)

C. Cryptology (CRYPTO)

D. Key Exchange Algorithm (KEA)

Correct Answer: C

Explanation

Explanation/Reference:
Explanation: Cryptology is the science that includes both cryptography and cryptanalysis and is not directly concerned with key management. Cryptology is the mathematics, such as number theory, and the application of formulas and algorithms, that underpin cryptography and cryptanalysis.
The following are all concerned with Key Management which makes them the wrong choices:
Internet Security Association Key Management Protocol (ISAKMP) is a key management protocol used by IPSec. ISAKMP (Internet Security Association and Key Management Protocol) is a protocol defined by RFC 2408 for establishing Security Associations (SA) and cryptographic keys in an Internet environment. ISAKMP only provides a framework for authentication and key exchange. The actual key exchange is done by the Oakley Key Determination Protocol which is a key-agreement protocol that allows authenticated parties to exchange keying material across an insecure connection using the Diffie-Hellman key exchange algorithm. Diffie-Hellman and one variation of the Diffie-Hellman algorithm called the Key Exchange Algorithm (KEA) are also key exchange protocols. Key exchange (also known as "key establishment") is any method in cryptography by which cryptographic keys are exchanged between users, allowing use of a cryptographic algorithm. DiffieHellman key exchange (DH) is a specific method of exchanging keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The DiffieHellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.
Reference(s) used for this question:
Mike Meyers CISSP Certification Passport, by Shon Harris and Mike Meyers, page 228. It is highlighted as an EXAM TIP. Which tells you that it is a must know for the purpose of the exam.
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, Fifth Edition, Chapter 8: Cryptography (page 713-715).
and
https://en.wikipedia.org/wiki/ISAKMP
and
http://searchsecurity.techtarget.com/definition/cryptology

QUESTION 178
Which of the following encryption algorithms does not deal with discrete logarithms?

A. El Gamal
B. Diffie-Hellman
C. RSA
D. Elliptic Curve

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The security of the RSA system is based on the assumption that factoring the product into two original large prime numbers is difficult Source:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 159). Shon Harris, CISSP All-in-One Examine Guide, Third Edition, McGraw-Hill Companies, August 2005, Chapter 8: Cryptography, Page 636 - 639

QUESTION 179
Which of the following statements pertaining to message digests is incorrect?

A. The original file cannot be created from the message digest.
B. Two different files should not have the same message digest.
C. The message digest should be calculated using at least 128 bytes of the file.
D. Messages digests are usually of fixed size.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 160).

QUESTION 180
Which type of attack is based on the probability of two different messages using the same hash function producing a common message digest?

A. Differential cryptanalysis
B. Differential linear cryptanalysis
C. Birthday attack
D. Statistical attack

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: A Birthday attack is usually applied to the probability of two different messages using the same hash function producing a common message digest. The term "birthday" comes from the fact that in a room with 23 people, the probability of two of more people having the same birthday is greater than 50%. Linear cryptanalysis is a general form of cryptanalysis based on finding affine approximations to the action of a cipher. Attacks have been developed for block ciphers and stream ciphers. Linear cryptanalysis is one of the two most widely used attacks on block ciphers; the other being differential cryptanalysis.
Differential Cryptanalysis is a potent cryptanalytic technique introduced by Biham and Shamir. Differential cryptanalysis is designed for the study and attack of DES-like cryptosystems. A DESISC SSCP Exam
like cryptosystem is an iterated cryptosystem which relies on conventional cryptographic techniques such as substitution and diffusion.
Differential cryptanalysis is a general form of cryptanalysis applicable primarily to block ciphers, but also to stream ciphers and cryptographic hash functions. In the broadest sense, it is the study of how differences in an input can affect the resultant difference at the output. In the case of a block cipher, it refers to a set of techniques for tracing differences through the network of transformations, discovering where the cipher exhibits non-random behaviour, and exploiting such properties to recover the secret key.
Source:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 163).
and
http://en.wikipedia.org/wiki/Differential_cryptanalysis

QUESTION 181
Which of the following elements is NOT included in a Public Key Infrastructure (PKI)?

A. Timestamping
B. Repository
C. Certificate revocation
D. Internet Key Exchange (IKE)

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Other elements are included in a PKI.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 165).

QUESTION 182
Which of the following was developed in order to protect against fraud in electronic fund transfers (EFT) by ensuring the message comes from its claimed originator and that it has not been altered in transmission?

A. Secure Electronic Transaction (SET)
B. Message Authentication Code (MAC)
C. Cyclic Redundancy Check (CRC)
D. Secure Hash Standard (SHS)

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: In order to protect against fraud in electronic fund transfers (EFT), the Message Authentication Code (MAC), ANSI X9.9, was developed. The MAC is a check value, which is derived from the contents of the message itself, that is sensitive to the bit changes in a message.
It is similar to a Cyclic Redundancy Check (CRC).
The aim of message authentication in computer and communication systems is to verify that he message comes from its claimed originator and that it has not been altered in transmission. It is particularly needed for EFT Electronic Funds Transfer). The protection mechanism is generation of a Message Authentication Code (MAC), attached to the message, which can be recalculated by the receiver and will reveal any alteration in transit. One standard method is described in (ANSI, X9.9). Message authentication mechanisms an also be used to achieve non-repudiation of messages.
The Secure Electronic Transaction (SET) was developed by a consortium including MasterCard and VISA as a means of preventing fraud from occurring during electronic payment. The Secure Hash Standard (SHS), NIST FIPS 180, available at http://www.itl.nist.gov/fipspubs/fip180-1.htm, specifies the Secure Hash Algorithm (SHA-1).
Source:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 170) also see:
http://luizfirmino.blogspot.com/2011/04/message-authentication-code-mac.html and
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.22.2312&rep=rep1&type=pdf

QUESTION 183
Which of the following statements pertaining to Secure Sockets Layer (SSL) is false?

A. The SSL protocol was developed by Netscape to secure Internet client-server transactions.
B. The SSL protocol's primary use is to authenticate the client to the server using public key cryptography and digital certificates.
C. Web pages using the SSL protocol start with HTTPS
D. SSL can be used with applications such as Telnet, FTP and email protocols.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: All of these statements pertaining to SSL are true except that it is primary use is to authenticate the client to the server using public key cryptography and digital certificates. It is the opposite, Its primary use is to authenticate the server to the client. The following reference(s) were used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 170).

QUESTION 184
What is the name of the protocol use to set up and manage Security Associations (SA) for IP Security (IPSec)?

A. Internet Key Exchange (IKE)

B. Secure Key Exchange Mechanism

C. Oakley

D. Internet Security Association and Key Management Protocol

Correct Answer: A

Explanation

Explanation/Reference:

Explanation: The Key management for IPSec is called the Internet Key Exchange (IKE) Note: IKE underwent a series of improvements establishing IKEv2 with RFC 4306. The basis of this answer is IKEv2.

The IKE protocol is a hybrid of three other protocols: ISAKMP (Internet Security Association and Key Management Protocol), Oakley and SKEME. ISAKMP provides a framework for authentication and key exchange, but does not define them (neither authentication nor key exchange). The Oakley protocol describes a series of modes for key exchange and the SKEME protocol defines key exchange techniques.

IKE--Internet Key Exchange. A hybrid protocol that implements Oakley and Skeme key exchanges inside the ISAKMP framework. IKE can be used with other protocols, but its initial implementation is with the IPSec protocol. IKE provides authentication of the IPSec peers, negotiates IPSec keys, and negotiates IPSec security associations. IKE is implemented in accordance with RFC 2409, The Internet Key Exchange. The Internet Key Exchange (IKE) security protocol is a key management protocol standard that is used in conjunction with the IPSec standard. IPSec can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard.

IKE is a hybrid protocol that implements the Oakley key exchange and the SKEME key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. (ISAKMP, Oakley, and SKEME are security protocols implemented by IKE.) IKE automatically negotiates IPSec security associations (SAs) and enables IPSec secure communications without costly manual preconfiguration. Specifically, IKE provides these benefits:

·Eliminates the need to manually specify all the IPSec security parameters in the crypto maps at both peers.

·Allows you to specify a lifetime for the IPSec security association. ·Allows encryption keys to change during IPSec sessions.

·Allows IPSec to provide anti-replay services.

·Permits certification authority (CA) support for a manageable, scalable IPSec implementation.

·Allows dynamic authentication of peers.

About ISAKMP

The Internet Security Association and Key Management Protocol (ISAKMP) is a framework that defines the phases for establishing a secure relationship and support for negotiation of security attributes, it does not establish sessions keys by itself, it is used along with the Oakley session key establishment protocol. The Secure Key Exchange Mechanism (SKEME) describes a secure exchange mechanism and Oakley defines the modes of operation needed to establish a secure connection.

ISAKMP provides a framework for Internet key management and provides the specific protocol support for negotiation of security attributes. Alone, it does not establish session keys. However it can be used with various session key establishment protocols, such as Oakley, to provide a complete solution to Internet key management.

About Oakley

The Oakley protocol uses a hybrid Diffie-Hellman technique to establish session keys on Internet hosts and routers. Oakley provides the important security property of Perfect Forward Secrecy (PFS) and is based on cryptographic techniques that have survived substantial public scrutiny. Oakley can be used by itself, if no attribute negotiation is needed, or Oakley can be used in conjunction with ISAKMP. When ISAKMP is used with Oakley, key escrow is not feasible. The ISAKMP and Oakley protocols have been combined into a hybrid protocol. The resolution of ISAKMP with Oakley uses the framework of ISAKMP to support a subset of Oakley key exchange modes. This new key exchange protocol provides optional PFS, full security association attribute negotiation, and authentication methods that provide both repudiation and non-repudiation. Implementations of this protocol can be used to establish VPNs and also allow for users from remote sites (who may have a dynamically allocated IP address) access to a secure network.

About IPSec

The IETF's IPSec Working Group develops standards for IP-layer security mechanisms for both IPv4 and IPv6. The group also is developing generic key management protocols for use on the Internet. For more information, refer to the IP Security and Encryption Overview. IPSec is a framework of open standards developed by the Internet Engineering Task Force (IETF) that provides security for transmission of sensitive information over

unprotected networks such as the Internet. It acts at the network level and implements the following standards:
IPSec
Internet Key Exchange (IKE)
Data Encryption Standard (DES)
MD5 (HMAC variant)
SHA (HMAC variant)
Authentication Header (AH)
Encapsulating Security Payload (ESP)
IPSec services provide a robust security solution that is standards-based. IPSec also provides data authentication and anti-replay services in addition to data confidentiality services. For more information regarding IPSec, refer to the chapter "Configuring IPSec Network Security." About SKEME
SKEME constitutes a compact protocol that supports a variety of realistic scenarios and security models over Internet. It provides clear tradeoffs between security and performance as required by the different scenarios without incurring in unnecessary system complexity. The protocol supports key exchange based on public key, key distribution centers, or manual installation, and provides for fast and secure key refreshment. In addition, SKEME selectively provides perfect forward secrecy, allows for replaceability and negotiation of the underlying cryptographic primitives, and addresses privacy issues as anonymity and repudiatability SKEME's basic mode is based on the use of public keys and a Diffie-Hellman shared secret generation.
However, SKEME is not restricted to the use of public keys, but also allows the use of a preshared key. This key can be obtained by manual distribution or by the intermediary of a key distribution center (KDC) such as Kerberos.
In short, SKEME contains four distinct modes:
Basic mode, which provides a key exchange based on public keys and ensures PFS thanks to Diffie-Hellman. A key exchange based on the use of public keys, but without Diffie-Hellman. A key exchange based on the use of a pre-shared key and on Diffie-Hellman. A mechanism of fast rekeying based only on symmetrical algorithms. In addition, SKEME is composed of three phases: SHARE, EXCH and AUTH. During the SHARE phase, the peers exchange half-keys, encrypted with their respective public keys. These two half-keys are used to compute a secret key K. If anonymity is wanted, the identities of the two peers are also encrypted. If a shared secret already exists, this phase is skipped.
The exchange phase (EXCH) is used, depending on the selected mode, to exchange either Diffie- Hellman public values or nonces. The Diffie-Hellman shared secret will only be computed after the end of the exchanges.
The public values or nonces are authenticated during the authentication phase (AUTH), using the secret key established during the SHARE phase.
The messages from these three phases do not necessarily follow the order described above; in actual practice they are combined to minimize the number of exchanged messages.
References used for this question:
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 172).
http://tools.ietf.org/html/rfc4306
http://tools.ietf.org/html/rfc4301
http://en.wikipedia.org/wiki/Internet_Key_Exchange
CISCO ISAKMP and OAKLEY information
CISCO Configuring Internet Key Exchange Protocol
http://www.hsc.fr/ressources/articles/ipsec-tech/index.html.en

QUESTION 185
Which of the following binds a subject name to a public key value?

A. A public-key certificate
B. A public key infrastructure
C. A secret key infrastructure
D. A private key certificate

Correct Answer: A
Explanation

Explanation/Reference:

Explanation: Remember the term Public-Key Certificate is synonymous with Digital Certificate or Identity certificate.
The certificate itself provides the binding but it is the certificate authority who will go through the Certificate Practice Statements (CPS) actually validating the bindings and vouch for the identity of the owner of the key within the certificate.
As explained in Wikipedia:
In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document which uses a digital signature to bind together a public key with an identity -- information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual. In a typical public key infrastructure (PKI) scheme, the signature will be of a certificate authority (CA). In a web of trust scheme such as PGP or GPG, the signature is of either the user (a selfsigned certificate) or other users ("endorsements") by getting people to sign each other keys. In either case, the signatures on a certificate are attestations by the certificate signer that the identity information and the public key belong together.
RFC 2828 defines the certification authority (CA) as:
An entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate.
An authority trusted by one or more users to create and assign certificates. Optionally, the certification authority may create the user's keys.
X509 Certificate users depend on the validity of information provided by a certificate. Thus, a CA should be someone that certificate users trust, and usually holds an official position created and granted power by a government, a corporation, or some other organization. A CA is responsible for managing the life cycle of certificates and, depending on the type of certificate and the CPS that applies, may be responsible for the life cycle of key pairs associated with the certificates Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.
and
http://en.wikipedia.org/wiki/Public_key_certificate

QUESTION 186
What can be defined as a digital certificate that binds a set of descriptive data items, other than a public key, either directly to a subject name or to the identifier of another certificate that is a publickey certificate?

A. A public-key certificate
B. An attribute certificate
C. A digital certificate
D. A descriptive certificate

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The Internet Security Glossary (RFC2828) defines an attribute certificate as a digital certificate that binds a set of descriptive data items, other than a public key, either directly to a subject name or to the identifier of another certificate that is a public-key certificate. A public-key certificate binds a subject name to a public key value, along with information needed to perform certain cryptographic functions. Other attributes of a subject, such as a security clearance, may be certified in a separate kind of digital certificate, called an attribute certificate. A subject may have multiple attribute certificates associated with its name or with each of its public-key certificates. Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 187
What can be defined as a data structure that enumerates digital certificates that were issued to CAs but have been invalidated by their issuer prior to when they were scheduled to expire?

A. Certificate revocation list
B. Certificate revocation tree
C. Authority revocation list
D. Untrusted certificate list

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The Internet Security Glossary (RFC2828) defines the Authority Revocation List (ARL) as a data structure that enumerates digital certificates that were issued to CAs but have been invalidated by their issuer prior to when they were scheduled to expire. Do not to confuse with an ARL with a Certificate Revocation List (CRL). A certificate revocation list is a mechanism for distributing notices of certificate revocations. The question specifically mentions "issued to CAs" which makes ARL a better answer than CRL. http://rfclibrary.hosting.com/rfc/rfc2828/rfc2828-29.asp $ certificate revocation list (CRL)
(I) A data structure that enumerates digital certificates that have been invalidated by their issuer prior to when they were
scheduled to expire. (See: certificate expiration, X.509 certificate revocation list.) http://rfclibrary.hosting.com/rfc/rfc2828/rfc2828-17.asp $ authority revocation list (ARL)
(I) A data structure that enumerates digital certificates that were issued to CAs but have been invalidated by their issuer prior to when they were scheduled to expire. (See: certificate expiration, X.509 authority revocation list.)
In a few words: We use CRL's for end-user cert revocation and ARL's for CA cert revocation - both can be placed in distribution points.

QUESTION 188
What is the name of the third party authority that vouches for the binding between the data items in a digital certificate?

A. Registration authority
B. Certification authority
C. Issuing authority
D. Vouching authority

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: A certification authority (CA) is a third party entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate. An issuing authority could be considered a correct answer, but not the best answer, since it is too generic.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 189
What enables users to validate each other's certificate when they are certified under different certification hierarchies?

A. Cross-certification
B. Multiple certificates
C. Redundant certification authorities
D. Root certification authorities

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Cross-certification is the act or process by which two CAs each certifiy a public key of the other, issuing a public-key certificate to that other CA, enabling users that are certified under different certification hierarchies to validate each other's certificate. Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 190
Which of the following would best define a digital envelope?

A. A message that is encrypted and signed with a digital certificate.
B. A message that is signed with a secret key and encrypted with the sender's private key.
C. A message encrypted with a secret key attached with the message. The secret key is encrypted with the public key of the receiver.
D. A message that is encrypted with the recipient's public key and signed with the sender's private key.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: A digital envelope for a recipient is a combination of encrypted data and its encryption key in an encrypted form that has been prepared for use of the recipient. It consists of a hybrid encryption scheme in sealing a message, by encrypting the data and sending both it and a protected form of the key to the intended recipient, so that one else can open the message.
In PKCS #7, it means first encrypting the data using a symmetric encryption algorithm and a secret key, and then encrypting the secret key using an asymmetric encryption algorithm and the public key of the intended recipient.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 191
What can be defined as a value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity?

A. A digital envelope
B. A cryptographic hash
C. A Message Authentication Code
D. A digital signature

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: RFC 2828 (Internet Security Glossary) defines a digital signature as a value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity. The steps to create a Digital Signature are very simple:
1. You create a Message Digest of the message you wish to send
2. You encrypt the message digest using your Private Key which is the action of Signing
3. You send the Message along with the Digital Signature to the recipient To validate the Digital Signature the recipient will make use of the sender Public Key. Here are the steps:
1. The receiver will decrypt the Digital Signature using the sender Publick Key producing a clear text message digest.
2. The receiver will produce his own message digest of the message received.
3. At this point the receiver will compare the two message digest (the one sent and the one produce by the receiver), if the two matches, it proves the authenticity of the message and it confirms that the message was not modified in transit validating the integrity as well. Digital Signatures provides for Authenticity and Integrity only. There is no confidentiality in place, if you wish to get confidentiality it would be needed for the sender to encrypt everything with the receiver public key as a last step before sending the message.
A Digital Envelope is a combination of encrypted data and its encryption key in an encrypted form that has been prepared for use of the recipient. In simple term it is a type of security that uses two layers of encryption to protect a message. First, the message itself is encoded using symmetric encryption, and then the key to decode the message is encrypted using public-key encryption. This technique overcomes one of the problems of public-key encryption, which is that it is slower than symmetric encryption. Because only the key is protected with public-key encryption, there is very little overhead.
A cryptographic hash is the result of a cryptographic hash function such as MD5, SHA-1, or SHA-

2. A hash value also called a Message Digest is like a fingerprint of a message. It is used to proves integrity and ensure the message was not changed either in transit or in storage. A Message Authentication Code (MAC) refers to an ANSI standard for a checksum that is computed with a keyed hash that is based on DES or it can also be produced without using DES by concataning the Secret Key at the end of the message (simply adding it at the end of the message) being sent and then producing a Message digest of the Message+Secret Key together. The MAC is then attached and sent along with the message but the Secret Key is NEVER sent in clear text over the network.
In cryptography, HMAC (Hash-based Message Authentication Code), is a specific construction for calculating a message authentication code (MAC) involving a cryptographic hash function in combination with a secret key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authenticity of a message. Any cryptographic hash function, such as MD5 or SHA-1, may be used in the calculation of an HMAC; the resulting MAC algorithm is termed HMACMD5 or HMAC-SHA1 accordingly. The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, the size of its hash output length in bits and on the size and quality of the cryptographic key.
There is more than one type of MAC: Meet CBC-MAC
In cryptography, a Cipher Block Chaining Message Authentication Code, abbreviated CBC-MAC, is a technique for constructing a message authentication code from a block cipher. The message is encrypted with some block cipher algorithm in CBC mode to create a chain of blocks such that each block depends on the proper encryption of the previous block. This interdependence ensures that a change to any of the plaintext bits will cause the final encrypted block to change in a way that cannot be predicted or counteracted without knowing the key to the block cipher.

SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.
and
http://www.webopedia.com/TERM/D/digital_envelope.html
and
http://en.wikipedia.org/wiki/CBC-MAC

QUESTION 192
Which of the following can be best defined as computing techniques for inseparably embedding unobtrusive marks or labels as bits in digital data and for detecting or extracting the marks later?

A. Steganography
B. Digital watermarking
C. Digital enveloping
D. Digital signature

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: RFC 2828 (Internet Security Glossary) defines digital watermarking as computing techniques for inseparably embedding unobtrusive marks or labels as bits in digital data-text, graphics, images, video, or audio#and for detecting or extracting the marks later. The set of embedded bits (the digital watermark) is sometimes hidden, usually imperceptible, and always intended to be unobtrusive. It is used as a measure to protect intellectual property rights. Steganography involves hiding the very existence of a message. A digital signature is a value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity. A digital envelope is a combination of encrypted data and its encryption key in an encrypted form that has been prepared for use of the recipient.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 193
Which of the following is an Internet IPsec protocol to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism?

A. OAKLEY
B. Internet Security Association and Key Management Protocol (ISAKMP)
C. Simple Key-management for Internet Protocols (SKIP)
D. IPsec Key exchange (IKE)

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: RFC 2828 (Internet Security Glossary) defines the Internet Security Association and Key Management Protocol (ISAKMP) as an Internet IPsec protocol to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism.
Let's clear up some confusion here first. Internet Key Exchange (IKE) is a hybrid protocol, it consists of 3 "protocols"
ISAKMP: It's not a key exchange protocol per se, it's a framework on which key exchange protocols operate. ISAKMP is part of IKE. IKE establishs the shared security policy and authenticated keys. ISAKMP is the protocol that specifies the mechanics of the key exchange. Oakley: Describes the "modes" of key exchange (e.g. perfect forward secrecy for keys, identity protection, and authentication). Oakley describes a series of key exchanges and services. SKEME: Provides support for public-key-based key exchange, key distribution centres, and manual installation, it also outlines methods of secure and fast key refreshment. So yes, IPSec does use IKE, but ISAKMP is part of IKE. The questions did not ask for the actual key negotiation being done but only for the "exchange of key generation and authentication data" being done. Under Oakly it would be Diffie Hellman (DH) that would be used for the actual key nogotiation.
The following are incorrect answers:
Simple Key-management for Internet Protocols (SKIP) is a key distribution protocol that uses hybrid encryption to convey session keys that are used to encrypt data in IP packets. OAKLEY is a key establishment protocol (proposed for IPsec but superseded by IKE) based on the Diffie-Hellman algorithm and designed to be a compatible component of ISAKMP. IPsec Key Exchange (IKE) is an Internet, IPsec, key-establishment protocol [R2409] (partly based on OAKLEY) that is intended for putting in place authenticated keying material for use with ISAKMP and for other security associations, such as in AH and ESP.
Reference used for this question:
SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 194
Which of the following is defined as a key establishment protocol based on the Diffie-Hellman algorithm proposed for IPsec but superseded by IKE?

A. Diffie-Hellman Key Exchange Protocol
B. Internet Security Association and Key Management Protocol (ISAKMP)
C. Simple Key-management for Internet Protocols (SKIP)
D. OAKLEY

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: RFC 2828 (Internet Security Glossary) defines OAKLEY as a key establishment protocol (proposed for IPsec but superseded by IKE) based on the Diffie-Hellman algorithm and designed to be a compatible component of ISAKMP.
ISAKMP is an Internet IPsec protocol to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism.
SKIP is a key distribution protocol that uses hybrid encryption to convey session keys that are used to encrypt data in IP packets.
ISAKMP provides a framework for authentication and key exchange but does not define them. ISAKMP is

designed to be key exchange independant; that is, it is designed to support many different key exchanges. Oakley and SKEME each define a method to establish an authenticated key exchange. This includes payloads construction, the information payloads carry, the order in which they are processed and how they are used. Oakley describes a series of key exchanges-- called modes and details the services provided by each (e.g. perfect forward secrecy for keys, identity protection, and authentication). SKEME describes a versatile key exchange technique which provides anonymity, repudiability, and quick key refreshment.
RFC 2049 describes the IKE protocol using part of Oakley and part of SKEME in conjunction with ISAKMP to obtain authenticated keying material for use with ISAKMP, and for other security associations such as AH and ESP for the IETF IPsec DOI. While Oakley defines "modes", ISAKMP defines "phases". The relationship between the two is very straightforward and IKE presents different exchanges as modes which operate in one of two phases.
Phase 1 is where the two ISAKMP peers establish a secure, authenticated channel with which to communicate. This is called the ISAKMP Security Association (SA). "Main Mode" and "Aggressive Mode" each accomplish a phase 1 exchange. "Main Mode" and "Aggressive Mode" MUST ONLY be used in phase 1.
Phase 2 is where Security Associations are negotiated on behalf of services such as IPsec or any other service which needs key material and/or parameter negotiation. "Quick Mode" accomplishes a phase 2 exchange. "Quick Mode" MUST ONLY be used in phase 2.
CISSP: Certified Information Systems Security Professional Study Guide By James Michael Stewart, Ed Tittel, Mike Chappl, page 397
RFC 2049 at: http://www.ietf.org/rfc/rfc2409
SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000. The All-in-one CISSP Exam Guide, 3rd Edition, by Shon Harris, page 674 The CISSP and CAP Prep Guide, Platinum Edition, by Krutz and Vines

QUESTION 195
Which of the following is defined as an Internet, IPsec, key-establishment protocol, partly based on OAKLEY, that is intended for putting in place authenticated keying material for use with ISAKMP and for other security associations?

A. Internet Key exchange (IKE)
B. Security Association Authentication Protocol (SAAP)
C. Simple Key-management for Internet Protocols (SKIP)
D. Key Exchange Algorithm (KEA)

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: RFC 2828 (Internet Security Glossary) defines IKE as an Internet, IPsec, keyestablishment protocol (partly based on OAKLEY) that is intended for putting in place authenticated keying material for use with ISAKMP and for other security associations, such as in AH and ESP.
The following are incorrect answers:
SKIP is a key distribution protocol that uses hybrid encryption to convey session keys that are used to encrypt data in IP packets.
The Key Exchange Algorithm (KEA) is defined as a key agreement algorithm that is similar to the Diffie-Hellman algorithm, uses 1024-bit asymmetric keys, and was developed and formerly classified at the secret level by the NSA.
Security Association Authentication Protocol (SAAP) is a distracter.
Reference(s) used for this question:
SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 196
Which of the following can best be defined as a key distribution protocol that uses hybrid encryption to convey session keys. This protocol establishes a long-term key once, and then requires no prior communication in order to establish or exchange keys on a session-by-session basis?

A. Internet Security Association and Key Management Protocol (ISAKMP)
B. Simple Key-management for Internet Protocols (SKIP)

C. Diffie-Hellman Key Distribution Protocol

D. IPsec Key exchange (IKE)

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: RFC 2828 (Internet Security Glossary) defines Simple Key Management for Internet Protocols (SKIP) as:
A key distribution protocol that uses hybrid encryption to convey session keys that are used to encrypt data in IP packets.
SKIP is an hybrid Key distribution protocol similar to SSL, except that it establishes a long-term key once, and then requires no prior communication in order to establish or exchange keys on a session-by-session basis. Therefore, no connection setup overhead exists and new keys values are not continually generated. SKIP uses the knowledge of its own secret key or private component and the destination's public component to calculate a unique key that can only be used between them.
IKE stand for Internet Key Exchange, it makes use of ISAKMP and OAKLEY internally. Internet Key Exchange (IKE or IKEv2) is the protocol used to set up a security association (SA) in the IPsec protocol suite. IKE builds upon the Oakley protocol and ISAKMP. IKE uses X.509 certificates for authentication and a DiffieHellman key exchange to set up a shared session secret from which cryptographic keys are derived.
The following are incorrect answers:
ISAKMP is an Internet IPsec protocol to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism.
IKE is an Internet, IPsec, key-establishment protocol (partly based on OAKLEY) that is intended for putting in place authenticated keying material for use with ISAKMP and for other security associations, such as in AH and ESP.
IPsec Key exchange (IKE) is only a detracto.
Reference(s) used for this question:
SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.
and
http://en.wikipedia.org/wiki/Simple_Key-Management_for_Internet_Protocol and
http://en.wikipedia.org/wiki/Simple_Key-Management_for_Internet_Protocol

QUESTION 197
Which of the following can best be defined as a cryptanalysis technique in which the analyst tries to determine the key from knowledge of some plaintext-ciphertext pairs?

A. A known-plaintext attack

B. A known-algorithm attack

C. A chosen-ciphertext attack

D. A chosen-plaintext attack

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: RFC2828 (Internet Security Glossary) defines a known-plaintext attack as a cryptanalysis technique in which the analyst tries to determine the key from knowledge of some plaintext-ciphertext pairs (although the analyst may also have other clues, such as the knowing the cryptographic algorithm). A chosen-ciphertext attack is defined as a cryptanalysis technique in which the analyst tries to determine the key from knowledge of plaintext that corresponds to ciphertext selected (i.e., dictated) by the analyst. A chosen-plaintext attack is a cryptanalysis technique in which the analyst tries to determine the key from knowledge of ciphertext that corresponds to plaintext selected (i.e., dictated) by the analyst. The other choice is a distracter.
The following are incorrect answers:
A chosen-plaintext attacks
The attacker has the plaintext and ciphertext, but can choose the plaintext that gets encrypted to see the corresponding ciphertext. This gives her more power and possibly a deeper understanding of the way the

encryption process works so she can gather more information about the key being used. Once the key is discovered, other messages encrypted with that key can be decrypted.
A chosen-ciphertext attack
In chosen-ciphertext attacks, the attacker can choose the ciphertext to be decrypted and has access to the resulting decrypted plaintext. Again, the goal is to figure out the key. This is a harder attack to carry out compared to the previously mentioned attacks, and the attacker may need to have control of the system that contains the cryptosystem.
A known-algorithm attack
Knowing the algorithm does not give you much advantage without knowing the key. This is a bogus detractor. The algorithm should be public, which is the Kerckhoffs's Principle . The only secret should be the key.
Reference(s) used for this question:
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.
and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 866). McGraw-Hill. Kindle Edition.
and
Kerckhoffs's Principle

QUESTION 198
Which of the following is NOT a property of a one-way hash function?

A. It converts a message of a fixed length into a message digest of arbitrary length.
B. It is computationally infeasible to construct two different messages with the same digest.
C. It converts a message of arbitrary length into a message digest of a fixed length.
D. Given a digest value, it is computationally infeasible to find the corresponding message.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: An algorithm that turns messages or text into a fixed string of digits, usually for security or data management purposes. The "one way" means that it's nearly impossible to derive the original text from the string.
A one-way hash function is used to create digital signatures, which in turn identify and authenticate the sender and message of a digitally distributed message. A cryptographic hash function is a deterministic procedure that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that an accidental or intentional change to the data will change the hash value. The data to be encoded is often called the "message," and the hash value is sometimes called the message digest or simply digest. The ideal cryptographic hash function has four main or significant properties:
it is easy (but not necessarily quick) to compute the hash value for any given message it is infeasible to generate a message that has a given hash it is infeasible to modify a message without changing the hash it is infeasible to find two different messages with the same hash Cryptographic hash functions have many information security applications, notably in digital signatures, message authentication codes (MACs), and other forms of authentication. They can also be used as ordinary hash functions, to index data in hash tables, for fingerprinting, to detect duplicate data or uniquely identify files, and as checksums to detect accidental data corruption. Indeed, in information security contexts, cryptographic hash values are sometimes called (digital) fingerprints, checksums, or just hash values, even though all these terms stand for functions with rather different properties and purposes.
Source:
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.
and
http://en.wikipedia.org/wiki/Cryptographic_hash_function

QUESTION 199
The Data Encryption Algorithm performs how many rounds of substitution and permutation?

A. 4
B. 16

C. 54

D. 64

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 200
Which of the following statements is most accurate regarding a digital signature?

A. It is a method used to encrypt confidential data.

B. It is the art of transferring handwritten signature to electronic media.

C. It allows the recipient of data to prove the source and integrity of data.

D. It can be used as a signature system and a cryptosystem.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 201
The computations involved in selecting keys and in enciphering data are complex, and are not practical for manual use. However, using mathematical properties of modular arithmetic and a method known as " ," RSA is quite feasible for computer use.

A. computing in Galois fields

B. computing in Gladden fields

C. computing in Gallipoli fields

D. computing in Galbraith fields

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The computations involved in selecting keys and in enciphering data are complex, and are not practical for manual use. However, using mathematical properties of modular arithmetic and a method known as computing in Galois fields, RSA is quite feasible for computer use.
Source: FITES, Philip E., KRATZ, Martin P., Information Systems Security: A Practitioner's Reference, 1993, Van Nostrand Reinhold, page 44.

QUESTION 202
Which of the following concerning the Rijndael block cipher algorithm is false?

A. The design of Rijndael was strongly influenced by the design of the block cipher Square.

B. A total of 25 combinations of key length and block length are possible

C. Both block size and key length can be extended to multiples of 64 bits.

D. The cipher has a variable block length and key length.

Correct Answer: C
Explanation

Explanation/Reference:

Explanation: The answer above is the correct answer because it is FALSE. Rijndael does not support multiples of 64 bits but multiples of 32 bits in the range of 128 bits to 256 bits. Key length could be 128, 160, 192, 224, and 256.
Both block length and key length can be extended very easily to multiples of 32 bits. For a total combination of 25 different block and key size that are possible.
The Rijndael Cipher
Rijndael is a block cipher, designed by Joan Daemen and Vincent Rijmen as a candidate algorithm for the Advanced Encryption Standard (AES) in the United States of America. The cipher has a variable block length and key length.
Rijndael can be implemented very efficiently on a wide range of processors and in hardware. The design of Rijndael was strongly influenced by the design of the block cipher Square.
The Advanced Encryption Standard (AES)
The Advanced Encryption Standard (AES) keys are defined to be either 128, 192, or 256 bits in accordance with the requirements of the AES.
The number of rounds, or iterations of the main algorithm, can vary from 10 to 14 within the Advanced Encryption Standard (AES) and is dependent on the block size and key length. 128 bits keys uses 10 rounds or encryptions, 192 bits keys uses 12 rounds of encryption, and 256 bits keys uses 14 rounds of encryption.
The low number of rounds has been one of the main criticisms of Rijndael, but if this ever becomes a problem the number of rounds can easily be increased at little extra cost performance wise by increasing the block size and key length.
Range of key and block lengths in Rijndael and AES
Rijndael and AES differ only in the range of supported values for the block length and cipher key length.
For Rijndael, the block length and the key length can be independently specified to any multiple of 32 bits, with a minimum of 128 bits, and a maximum of 256 bits. The support for block and key lengths 160 and 224 bits was introduced in Joan Daemen and Vincent Rijmen, AES submission document on Rijndael, Version 2, September 1999 available at http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf AES fixes the block length to 128 bits, and supports key lengths of 128, 192 or 256 bits only.
Reference used for this question:
The Rijndael Page
and
http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf and
FIPS PUB 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology, U.S. Department of Commerce, November 2001.

QUESTION 203
This type of attack is generally most applicable to public-key cryptosystems, what type of attack am I ?

A. Chosen-Ciphertext attack
B. Ciphertext-only attack
C. Plaintext Only Attack
D. Adaptive-Chosen-Plaintext attack

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: A chosen-ciphertext attack is one in which cryptanalyst may choose a piece of ciphertext and attempt to obtain the corresponding decrypted plaintext. This type of attack is generally most applicable to public-key cryptosystems. A chosen-ciphertext attack (CCA) is an attack model for cryptanalysis in which the cryptanalyst gathers information, at least in part, by choosing a ciphertext and obtaining its decryption under an unknown key. In the attack, an adversary has a chance to enter one or more known ciphertexts into the system and obtain the resulting plaintexts. From these pieces of information the adversary can attempt to recover the hidden secret key used for decryption. A number of otherwise secure schemes can be defeated under chosen-ciphertext attack. For example, the El Gamal cryptosystem is semantically secure under chosen-plaintext attack, but this semantic security can be trivially defeated under a chosen-ciphertext attack. Early versions of RSA padding used in the SSL protocol were vulnerable to a sophisticated adaptive chosen-ciphertext attack which revealed SSL session keys. Chosen-ciphertext attacks have implications for some self-synchronizing stream ciphers as well. Designers of tamper-resistant cryptographic smart cards must be particularly cognizant

of these attacks, as these devices may be completely under the control of an adversary, who can issue a large number of chosen-ciphertexts in an attempt to recover the hidden secret key.

According to RSA:

Cryptanalytic attacks are generally classified into six categories that distinguish the kind of information the cryptanalyst has available to mount an attack. The categories of attack are listed here roughly in increasing order of the quality of information available to the cryptanalyst, or, equivalently, in decreasing order of the level of difficulty to the cryptanalyst. The objective of the cryptanalyst in all cases is to be able to decrypt new pieces of ciphertext without additional information. The ideal for a cryptanalyst is to extract the secret key. A ciphertext-only attack is one in which the cryptanalyst obtains a sample of ciphertext, without the plaintext associated with it. This data is relatively easy to obtain in many scenarios, but a successful ciphertext-only attack is generally difficult, and requires a very large ciphertext sample. Such attack was possible on cipher using Code Book Mode where frequency analysis was being used and even thou only the ciphertext was available, it was still possible to eventually collect enough data and decipher it without having the key.

A known-plaintext attack is one in which the cryptanalyst obtains a sample of ciphertext and the corresponding plaintext as well. The known-plaintext attack (KPA) or crib is an attack model for cryptanalysis where the attacker has samples of both the plaintext and its encrypted version (ciphertext), and is at liberty to make use of them to reveal further secret information such as secret keys and code books.

A chosen-plaintext attack is one in which the cryptanalyst is able to choose a quantity of plaintext and then obtain the corresponding encrypted ciphertext. A chosen-plaintext attack (CPA) is an attack model for cryptanalysis which presumes that the attacker has the capability to choose arbitrary plaintexts to be encrypted and obtain the corresponding ciphertexts. The goal of the attack is to gain some further information which reduces the security of the encryption scheme. In the worst case, a chosen-plaintext attack could reveal the scheme's secret key. This appears, at first glance, to be an unrealistic model; it would certainly be unlikely that an attacker could persuade a human cryptographer to encrypt large amounts of plaintexts of the attacker's choosing. Modern cryptography, on the other hand, is implemented in software or hardware and is used for a diverse range of applications; for many cases, a chosen-plaintext attack is often very feasible. Chosen-plaintext attacks become extremely important in the context of public key cryptography, where the encryption key is public and attackers can encrypt any plaintext they choose.

Any cipher that can prevent chosen-plaintext attacks is then also guaranteed to be secure against known-plaintext and ciphertext-only attacks; this is a conservative approach to security. Two forms of chosen-plaintext attack can be distinguished:

Batch chosen-plaintext attack, where the cryptanalyst chooses all plaintexts before any of them are encrypted. This is often the meaning of an unqualified use of "chosen-plaintext attack". Adaptive chosen-plaintext attack, is a special case of chosen-plaintext attack in which the cryptanalyst is able to choose plaintext samples dynamically, and alter his or her choices based on the results of previous encryptions. The cryptanalyst makes a series of interactive queries, choosing subsequent plaintexts based on the information from the previous encryptions. Non-randomized (deterministic) public key encryption algorithms are vulnerable to simple "dictionary"-type attacks, where the attacker builds a table of likely messages and their corresponding ciphertexts. To find the decryption of some observed ciphertext, the attacker simply looks the ciphertext up in the table. As a result, public-key definitions of security under chosenplaintext attack require probabilistic encryption (i.e., randomized encryption). Conventional symmetric ciphers, in which the same key is used to encrypt and decrypt a text, may also be vulnerable to other forms of chosen-plaintext attack, for example, differential cryptanalysis of block ciphers.

An adaptive-chosen-ciphertext is the adaptive version of the above attack. A cryptanalyst can mount an attack of this type in a scenario in which he has free use of a piece of decryption hardware, but is unable to extract the decryption key from it. An adaptive chosen-ciphertext attack (abbreviated as CCA2) is an interactive form of chosenciphertext attack in which an attacker sends a number of ciphertexts to be decrypted, then uses the results of these decryptions to select subsequent ciphertexts. It is to be distinguished from an indifferent chosen-ciphertext attack (CCA1).

The goal of this attack is to gradually reveal information about an encrypted message, or about the decryption key itself. For public-key systems, adaptive-chosen-ciphertexts are generally applicable only when they have the property of ciphertext malleability -- that is, a ciphertext can be modified in specific ways that will have a predictable effect on the decryption of that message. A Plaintext Only Attack is simply a bogus detractor. If you have the plaintext only then there is no need to perform any attack.

RSA Laboratories FAQs about today's cryptography: What are some of the basic types of cryptanalytic attack?
also see:
http://www.giac.org/resources/whitepaper/cryptography/57.php and
http://en.wikipedia.org/wiki/Chosen-plaintext_attack

QUESTION 204
What is NOT true about a one-way hashing function?

A. It provides authentication of the message
B. A hash cannot be reverse to get the message used to create the hash
C. The results of a one-way hash is a message digest
D. It provides integrity of the message

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: A one way hashing function can only be use for the integrity of a message and not for authentication or confidentiality. Because the hash creates just a fingerprint of the message which cannot be reversed and it is also very difficult to create a second message with the same hash.
A hash by itself does not provide Authentication. It only provides a weak form or integrity. It would be possible for an attacker to perform a Man-In-The-Middle attack where both the hash and the digest could be changed without the receiver knowing it. A hash combined with your session key will produce a Message Authentication Code (MAC) which will provide you with both authentication of the source and integrity. It is sometimes referred to as a Keyed Hash.
A hash encrypted with the sender private key produce a Digital Signature which provide authentication, but not the hash by itself.
Hashing functions by themselves such as MD5, SHA1, SHA2, SHA-3 does not provide authentication.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, Page 548

QUESTION 205
You work in a police department forensics lab where you examine computers for evidence of crimes. Your work is vital to the success of the prosecution of criminals. One day you receive a laptop and are part of a two man team responsible for examining it together. However, it is lunch time and after receiving the laptop you leave it on your desk and you both head out to lunch.
What critical step in forensic evidence have you forgotten?

A. Chain of custody
B. Locking the laptop in your desk
C. Making a disk image for examination
D. Cracking the admin password with chntpw

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: When evidence from a crime is to be used in the prosecution of a criminal it is critical that you follow the law when handling that evidence. Part of that process is called chain of custody and is when you maintain proactive and documented control over ALL evidence involved in a crime.
Failure to do this can lead to the dismissal of charges against a criminal because if the evidence is compromised because you failed to maintain of chain of custody. A chain of custody is chronological documentation for evidence in a particular case, and is especially important with electronic evidence due to the possibility of fraudulent data alteration, deletion, or creation. A fully detailed chain of custody report is necessary to prove the physical custody of a piece of evidence and show all parties that had access to said evidence at any given time.
Evidence must be protected from the time it is collected until the time it is presented in court.
The following answers are incorrect:
- Locking the laptop in your desk: Even this wouldn't assure that the defense team would try to challenge chain of custody handling. It's usually easy to break into a desk drawer and evidence should be stored in approved safes or other storage facility.
- Making a disk image for examination: This is a key part of system forensics where we make a disk image of

the evidence system and study that as opposed to studying the real disk drive. That could lead to loss of evidence. However if the original evidence is not secured than the chain of custoday has not been maintained properly.
- Cracking the admin password with chntpw: This isn't correct. Your first mistake was to compromise the chain of custody of the laptop. The chntpw program is a Linux utility to (re)set the password of any user that has a valid (local) account on a Windows system, by modifying the crypted password in the registry's SAM file. You do not need to know the old password to set a new one. It works offline which means you must have physical access (i.e., you have to shutdown your computer and boot off a linux floppy disk). The bootdisk includes stuff to accessNTFS partitions and scripts to glue the whole thing together. This utility works with SYSKEY and includes the option to turn it off. A bootdisk image is provided on their website at http://freecode.com/projects/chntpw .
The following reference(s) was used to create this question:
For more details and to cover 100% of the exam question NO: s, subscribe to our holistic Security+ 2014 CBT Tutorial at: http://www.cccure.tv/
and
http://en.wikipedia.org/wiki/Chain_of_custody
and
http://www.datarecovery.com/forensic_chain_of_custody.asp

QUESTION 206
When we encrypt or decrypt data there is a basic operation involving ones and zeros where they are compared in a process that looks something like this:
0101 0001 Plain text
0111 0011 Key stream
0010 0010 Output
What is this cryptographic operation called?

A. Exclusive-OR

B. Bit Swapping

C. Logical-NOR

D. Decryption

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: When we encrypt data we are basically taking the plaintext information and applying some key material or keystream and conducting something called an XOR or Exclusive-OR operation.
The symbol used for XOR is the following: This is a type of cipher known as a stream cipher.
The operation looks like this:
0101 0001 Plain text
0111 0011 Key stream
0010 0010 Output (ciphertext)
As you can see, it's not simple addition and the XOR Operation uses something called a truth table that explains why 0+1=1 and 1+1=0.
The rules are simples, if both bits are the same the result is zero, if both bits are not the same the result is one.
The following answers are incorrect:
- Bit Swapping: Incorrect. This isn't a known cryptographic operations.
- Logical NOR: Sorry, this isn't correct but is where only 0+0=1. All other combinations of 1+1, 1+0 equals 0. More on NOR here.
- Decryption: Sorry, this is the opposite of the process of encryption or, the process of applying the keystream to the plaintext to get the resulting encrypted text. The following reference(s) was used to create this question:
For more details on XOR and all other question NO: s of cryptography. Subscribe to our holistic Security+ CBT tutorial at http://www.cccure.tv
and
http://en.wikipedia.org/wiki/Exclusive-or
and
http://en.wikipedia.org/wiki/Stream_cipher

QUESTION 207
Which type of encryption is considered to be unbreakable if the stream is truly random and is as large as the plaintext and never reused in whole or part?

A. One Time Pad (OTP)
B. One time Cryptopad (OTC)
C. Cryptanalysis
D. Pretty Good Privacy (PGP)

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: OTP or One Time Pad is considered unbreakable if the key is truly random and is as large as the plaintext and never reused in whole or part AND kept secret. In cryptography, a one-time pad is a system in which a key generated randomly is used only once to encrypt a message that is then decrypted by the receiver using the matching one-time pad and key. Messages encrypted with keys based on randomness have the advantage that there is theoretically no way to "break the code" by analyzing a succession of messages. Each encryption is unique and bears no relation to the next encryption so that some pattern can be detected. With a one-time pad, however, the decrypting party must have access to the same key used to encrypt the message and this raises the problem of how to get the key to the decrypting party safely or how to keep both keys secure. One-time pads have sometimes been used when the both parties started out at the same physical location and then separated, each with knowledge of the keys in the one-time pad. The key used in a one-time pad is called a secret key because if it is revealed, the messages encrypted with it can easily be deciphered. One-time pads figured prominently in secret message transmission and espionage before and during World War II and in the Cold War era. On the Internet, the difficulty of securely controlling secret keys led to the invention of public key cryptography. The biggest challenge with OTP was to get the pad security to the person or entity you wanted to communicate with. It had to be done in person or using a trusted courrier or custodian. It certainly did not scale up very well and it would not be usable for large quantity of data that needs to be encrypted as we often time have today.
The following answers are incorrect:
- One time Cryptopad: Almost but this isn't correct. Cryptopad isn't a valid term in cryptography.
- Cryptanalysis: Sorry, incorrect. Cryptanalysis is the process of analyzing information in an effort to breach the cryptographic security systems.
- PGP - Pretty Good Privacy: PGP, written by Phil Zimmermann is a data encryption and decryption program that provides cryptographic privacy and authentication for data. Still isn't the right answer though. Read more here about PGP.
The following reference(s) was used to create this question:
To get more info on this question NO: s or any question NO: s of Security+, subscribe to the CCCure Holistic Security+ CBT available at: http://www.cccure.tv and
http://users.telenet.be/d.rijmenants/en/otp.htm
and
http://en.wikipedia.org/wiki/One-time_pad
and
http://searchsecurity.techtarget.com/definition/one-time-pad

QUESTION 208
Which of the following answers is described as a random value used in cryptographic algorithms to ensure that patterns are not created during the encryption process?

A. IV - Initialization Vector
B. Stream Cipher
C. OTP - One Time Pad
D. Ciphertext

Correct Answer: A

Explanation

Explanation/Reference:
Explanation: The basic power in cryptography is randomness. This uncertainty is why encrypted data is unusable to someone without the key to decrypt. Initialization Vectors are a used with encryption keys to add an extra layer of randomness to encrypted data. If no IV is used the attacker can possibly break the keyspace because of patterns resulting in the encryption process. Implementation such as DES in Code Book Mode (CBC) would allow frequency analysis attack to take place.
In cryptography, an initialization vector (IV) or starting variable (SV)is a fixed-size input to a cryptographic primitive that is typically required to be random or pseudorandom. Randomization is crucial for encryption schemes to achieve semantic security, a property whereby repeated usage of the scheme under the same key does not allow an attacker to infer relationships between segments of the encrypted message. For block ciphers, the use of an IV is described by so-called modes of operation. Randomization is also required for other primitives, such as universal hash functions and message authentication codes based thereon.
It is define by TechTarget as:
An initialization vector (IV) is an arbitrary number that can be used along with a secret key for data encryption. This number, also called a nonce, is employed only one time in any session. The use of an IV prevents repetition in data encryption, making it more difficult for a hacker using a dictionary attack to find patterns and break a cipher. For example, a sequence might appear twice or more within the body of a message. If there are repeated sequences in encrypted data, an attacker could assume that the corresponding sequences in the message were also identical. The IV prevents the appearance of corresponding duplicate character sequences in the ciphertext.
The following answers are incorrect:
- Stream Cipher: This isn't correct. A stream cipher is a symmetric key cipher where plaintext digits are combined with pseudorandom key stream to product cipher text.
- OTP - One Time Pad: This isn't correct but OTP is made up of random values used as key material. (Encryption key) It is considered by most to be unbreakable but must be changed with a new key after it is used which makes it impractical for common use.
- Ciphertext: Sorry, incorrect answer. Ciphertext is basically text that has been encrypted with key material (Encryption key)
The following reference(s) was used to create this question:
For more details on this TOPIC and other question NO: s of the Security+ CBK, subscribe to our Holistic Computer Based Tutorial (CBT) at http://www.cccure.tv and
whatis.techtarget.com/definition/initialization-vector-IV and
en.wikipedia.org/wiki/Initialization_vector

QUESTION 209
Which of the following terms can be described as the process to conceal data into another file or media in a practice known as security through obscurity?

A. Steganography
B. ADS - Alternate Data Streams
C. Encryption
D. NTFS ADS

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: It is the art and science of encoding hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message or could claim there is a message.
It is a form of security through obscurity.
The word steganography is of Greek origin and means "concealed writing." It combines the Greek words steganos (), meaning "covered or protected," and graphei () meaning "writing." The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography, disguised as a book on magic. Generally, the hidden messages will appear to be (or be part of) something else: images, articles, shopping lists, or some other cover text. For example, the hidden message may be in invisible ink between the visible lines of a private letter.

The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable, will arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message. It is sometimes referred to as Hiding in Plain Sight. This image of trees blow contains in it another image of a cat using Steganography.

ADS Tree with Cat inside

Certki

This image below is hidden in the picture of the trees above:

Certki

Hidden Kitty
As explained here the image is hidden by removing all but the two least significant bits of each color component and subsequent normalization.
ABOUT MSF and LSF
One of the common method to perform steganography is by hiding bits within the Least Significant Bits of a media (LSB) or what is sometimes referred to as Slack Space. By modifying only the least significant bit, it is not possible to tell if there is an hidden message or not looking at the picture or the media. If you would change the Most Significant Bits (MSB) then it would be possible to view or detect the changes just by looking at the picture. A person can perceive only up to 6 bits of depth, bit that are changed past the first sixth bit of the color code would be undetectable to a human eye.
If we make use of a high quality digital picture, we could hide six bits of data within each of the pixel of the image. You have a color code for each pixel composed of a Red, Green, and Blue value. The color code is 3 sets of 8 bits each for each of the color. You could change the last two bit to hide your data. See below a color code for one pixel in binary format. The bits below are not real they are just example for illustration purpose:
RED GREEN BLUE
0101 0101 1100 1011 1110 0011
MSB LSB MSB LSB MSB LSB
Let's say that I would like to hide the letter A uppercase within the pixels of the picture. If we convert the letter "A" uppercase to a decimal value it would be number 65 within the ASCII table , in binary format the value 65 would translet to 01000001 You can break the 8 bits of character A uppercase in group of two bits as follow: 01 00 00 01 Using the pixel above we will hide those bits within the last two bits of each of the color as follow:
RED GREEN BLUE
0101 0101 1100 1000 1110 0000
MSB LSB MSB LSB MSB LSB
As you can see above, the last two bits of RED was already set to the proper value of 01, then we move to the GREEN value and we changed the last two bit from 11 to 00, and finally we changed the last two bits of blue to 00. One pixel allowed us to hide 6 bits of data. We would have to use another pixel to hide the remaining two bits.
The following answers are incorrect:
- ADS - Alternate Data Streams: This is almost correct but ADS is different from steganography in that ADS hides data in streams of communications or files while Steganography hides data in a single file.
- Encryption: This is almost correct but Steganography isn't exactly encryption as much as using space in a file to store another file.
- NTFS ADS: This is also almost correct in that you're hiding data where you have space to do so. NTFS, or New Technology File System common on Windows computers has a feature where you can hide files where they're not viewable under normal conditions. Tools are required to uncover the ADS-hidden files.
The following reference(s) was used to create this question:
The CCCure Security+ Holistic Tutorial at http://www.cccure.tv and
Steganography tool
and
http://en.wikipedia.org/wiki/Steganography

QUESTION 210
Which of the following type of cryptography is used when both parties use the same key to communicate securely with each other?

A. Symmetric Key Cryptography
B. PKI - Public Key Infrastructure
C. Diffie-Hellman
D. DSS - Digital Signature Standard

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Symmetric-key algorithms are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext (sender) and decryption of ciphertext (receiver). The keys

may be identical, in practice, they represent a shared secret between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption. This is also known as secret key encryption. In symmetric key cryptography, each end of the conversation must have the same key or they cannot decrypt the message sent to them by the other party. Symmetric key crypto is very fast but more difficult to manage due to the need to distribute the key in a secure means to all parts needing to decrypt the data. There is no key management built within Symmetric crypto.
PKI provides CIA - Confidentiality (Through encryption) Integrity (By guaranteeing that the message hasn't change in transit) and Authentication (Non-repudiation). Symmetric key crypto provides mostly Confidentiality.
The following answers are incorrect:
- PKI - Public Key Infrastructure: This is the opposite of symmetric key crypto. Each side in PKI has their own private key and public key. What one key encrypt the other one can decrypt. You make use of the receiver public key to communicate securely with a remote user. The receiver will use their matching private key to decrypt the data.
- Diffie-Hellman: Sorry, this is an asymmetric key technique. It is used for key agreement over an insecure network such as the Internet. It allows two parties who has never met to negotiate a secret key over an insecure network while preventing Man-In-The-Middle (MITM) attacks.
- DSS - Digital Signature Standard: Sorry, this is an asymmetric key technique. The following reference(s) was used to create this question:
To learn more about this question NO: s and 100% of the Security+ CBK, subscribe to our Holistic Computer Based Tutorial (CBT) on our Learning Management System at:
http://www.cccure.tv
and
http://en.wikipedia.org/wiki/Symmetric-key_algorithm

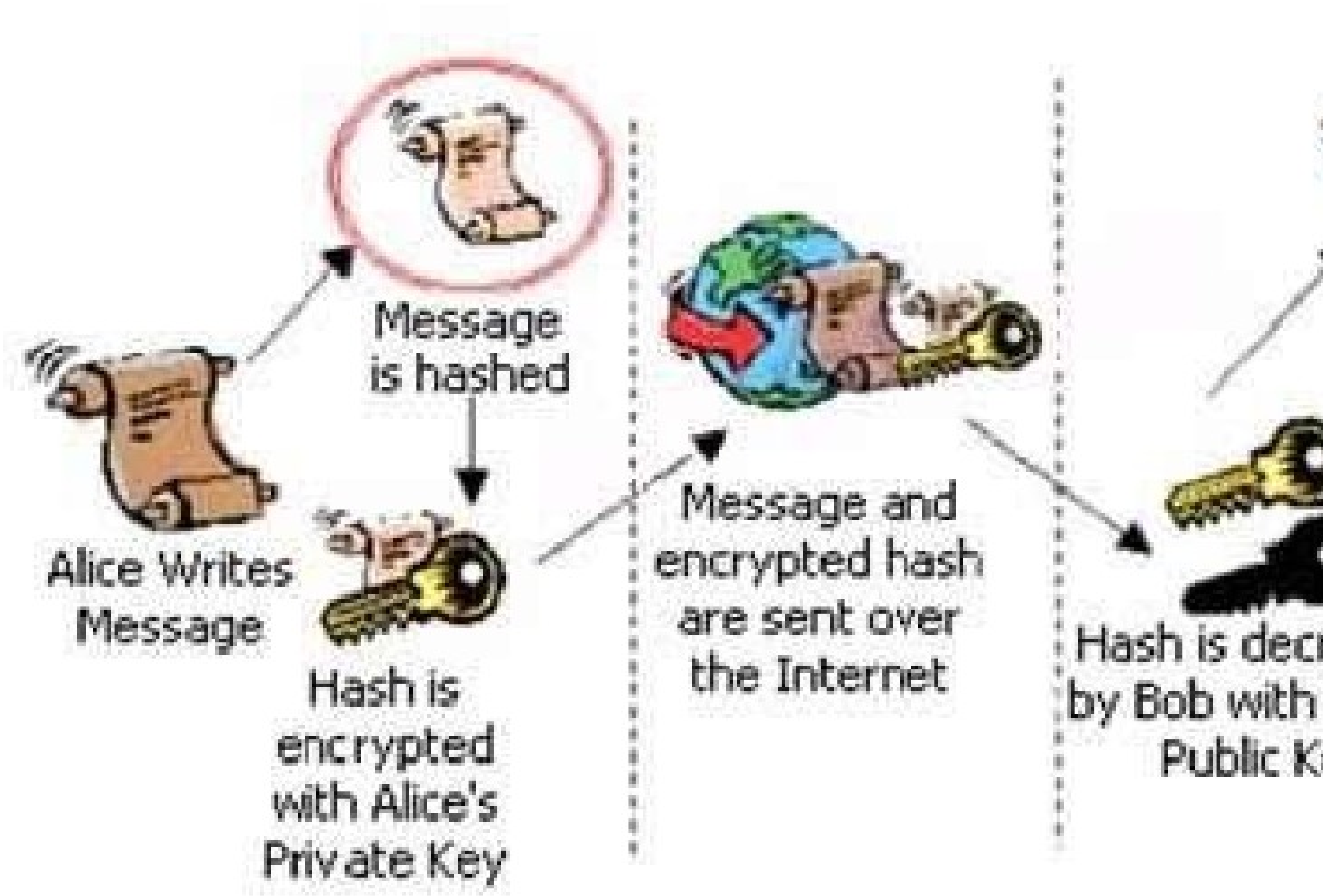
QUESTION 211
Complete the blanks. When using PKI, I digitally sign a message using my key. The recipient verifies my signature using my key.

A. Private / Public
B. Public / Private
C. Symmetric / Asymmetric
D. Private / Symmetric

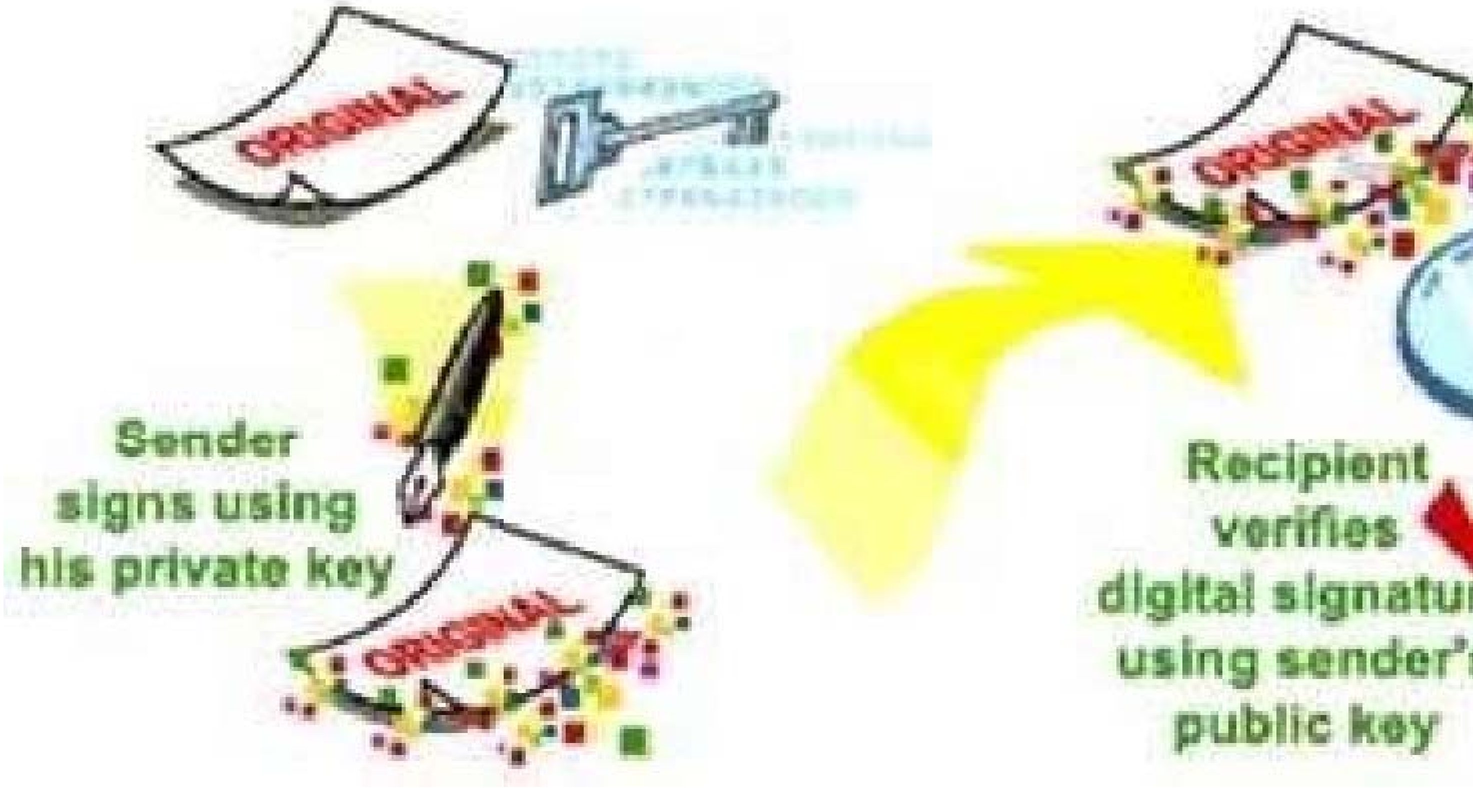
Correct Answer: A
Explanation

Explanation/Reference:
Explanation: When we encrypt messages using our private keys which are only available to us. The person who wants to read and decrypt the message need only have our public keys to do so. The whole point to PKI is to assure message integrity, authentication of the source, and to provide secrecy with the digital encryption.
See below a nice walktrough of Digital Signature creation and verification from the Comodo web site:
Digital Signatures apply the same functionality to an e-mail message or data file that a handwritten signature does for a paper-based document. The Digital Signature vouches for the origin and integrity of a message, document or other data file.
How do we create a Digital Signature?
The creation of a Digital Signature is a complex mathematical process. However as the complexities of the process are computed by the computer, applying a Digital Signature is no more difficult that creating a handwritten one!
The following text illustrates in general terms the processes behind the generation of a Digital Signature:
1. Alice clicks 'sign' in her email application or selects which file is to be signed.
2. Alice's computer calculates the 'hash' (the message is applied to a publicly known mathematical hashing function that coverts the message into a long number referred to as the hash).
3. The hash is encrypted with Alice's Private Key (in this case it is known as the Signing Key) to create the Digital Signature.
4. The original message and its Digital Signature are transmitted to Bob.
5. Bob receives the signed message. It is identified as being signed, so his email application knows which actions need to be performed to verify it.

6. Bob's computer decrypts the Digital Signature using Alice's Public Key.
7. Bob's computer also calculates the hash of the original message (remember - the mathematical function used by Alice to do this is publicly known).
8. Bob's computer compares the hashes it has computed from the received message with the now decrypted hash received with Alice's message.
digital signature creation and verification


Alice Writes Message
Message is hashed
Hash is encrypted with Alice's Private Key
Message and encrypted hash are sent over the Internet
Hash is dec
by Bob with
Public K

If the message has remained integral during its transit (i.e. it has not been tampered with), when compared the two hashes will be identical.
However, if the two hashes differ when compared then the integrity of the original message has been compromised. If the original message is tampered with it will result in Bob's computer calculating a different hash value. If a different hash value is created, then the original message will have been altered. As a result the verification of the Digital Signature will fail and Bob will be informed.
Origin, Integrity, Non-Repudiation, and Preventing Men-In-The-Middle (MITM) attacks Eve, who wants to impersonate Alice, cannot generate the same signature as Alice because she does not have Alice's Private Key (needed to sign the message digest). If instead, Eve decides to alter the content of the message while in transit, the tampered message will create a different message digest to the original message, and Bob's computer will be able to detect that. Additionally, Alice cannot deny sending the message as it has been signed using her Private Key, thus ensuring non-repudiation.
creating and validating a digital signature


ORIGINAL
Sender signs using his private key
ORIGINAL
ORIGINAL
Recipient verifies digital signatu
using sender's
public key

Due to the recent Global adoption of Digital Signature law, Alice may now sign a transaction, message or piece of digital data, and so long as it is verified successfully it is a legally permissible means of proof that Alice has made the transaction or written the message.
The following answers are incorrect:
- Public / Private: This is the opposite of the right answer.
- Symmetric / Asymmetric: Not quite. Sorry. This form of crypto is asymmetric so you were almost on target.
- Private / Symmetric: Well, you got half of it right but Symmetric is wrong. The following reference(s) was used to create this question:
The CCCure Holistic Security+ CBT, you can subscribe at: http://www.cccure.tv and http://www.comodo.com/resources/small-business/digital-certificates3.php

QUESTION 212
Which of the following BEST describes a function relying on a shared secret key that is used along with a hashing algorithm to verify the integrity of the communication content as well as the sender?

A. Message Authentication Code - MAC
B. PAM - Pluggable Authentication Module
C. NAM - Negative Acknowledgement Message
D. Digital Signature Certificate

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The purpose of a message authentication code - MAC is to verify both the source and message integrity without the need for additional processes. A MAC algorithm, sometimes called a keyed (cryptographic) hash function (however, cryptographic hash function is only one of the possible ways to generate MACs), accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC (sometimes known as a tag). The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the

message content.
MACs differ from digital signatures as MAC values are both generated and verified using the same secret key. This implies that the sender and receiver of a message must agree on the same key before initiating communications, as is the case with symmetric encryption. For the same reason, MACs do not provide the property of non-repudiation offered by signatures specifically in the case of a network-wide shared secret key: any user who can verify a MAC is also capable of generating MACs for other messages.
In contrast, a digital signature is generated using the private key of a key pair, which is asymmetric encryption. Since this private key is only accessible to its holder, a digital signature proves that a document was signed by none other than that holder. Thus, digital signatures do offer nonrepudiation.
The following answers are incorrect:
PAM - Pluggable Authentication Module: This isn't the right answer. There is no known message authentication function called a PAM. However, a pluggable authentication module (PAM) is a mechanism to integrate multiple low-level authentication schemes and commonly used within the Linux Operating System.
NAM - Negative Acknowledgement Message: This isn't the right answer. There is no known message authentication function called a NAM. The proper term for a negative acknowledgement is NAK, it is a signal used in digital communications to ensure that data is received with a minimum of errors.
Digital Signature Certificate: This isn't right. As it is explained and contrasted in the explanations provided above.
The following reference(s) was used to create this question:
The CCCure Computer Based Tutorial for Security+, you can subscribe at http://www.cccure.tv and http://en.wikipedia.org/wiki/Message_authentication_code

QUESTION 213
Which of the following type of traffic can easily be filtered with a stateful packet filter by enforcing the context or state of the request?

A. ICMP
B. TCP
C. UDP
D. IP

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The question is explict in asking *easily*. With TCP connection establishment there is a distinct state or sequence that can be expected. Consult the references for further details. ICMP, IP and UDP don't have any concept of a session; i.e. each packet or datagram is handled individually, with no reference to the contents of the previous one. With no sessions, these protocols usually cannot be filtered on the state of the session. Some newer firewalls, however, simulate the concept of state for these protocols, and filter out unexpected packets based upon normal usage. Although these are commonly treated like normal stateful filters, they are more complex to program, and hence more prone to errors. A stateful packet filter or stateful inspection inspects each packet and only allows known connection states through. So, if a SYN/ACK packet was recieved and there was not a prior SYN packet sent it would filter that packet and not let it in. The correct sequence of steps are known and if the sequence or state is incorrect then it is dropped.
The incorrect answers are:
ICMP. ICMP is basically stateless so you could not easily filter them based on the state or sequence.
UDP. UDP has no real state so you could only partially filter them based on the state or sequence. The question was explicit in asking easily. While it is possible, UDP is not the best answer. IP. IP would refer to the Internet Protocol and as such is stateless so you would not be able to filter it out easily.
The following reference(s) were used for this question:
http://www.nwo.net/ipf/ipf-howto.pdf

QUESTION 214
Which of the following access methods is used by Ethernet?

A. CSMA/CD.
B. CSU/DSU.

C. TCP/IP.

D. FIFO.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Ethernet uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) to minimize the effect of broadcast collisions.
The following answers are incorrect:
CSU/DSU Is incorrect because Channel Service Unit/Digital Service Unit(CSU/DSU) is a digital interface normally used to connect a router to a digital circuit. TCP/IP Is incorrect because Transmission Control Protocol/Internet Protocol(TCP/IP) is a network protocol not an access method.
FIFO Is incorrect as it is a distractor. First In, First Out (FIFO) is typically a processing methodology in which first come, first served.
Ethernet is a frame based network technology.
OIG CBK Telecommunications and Network Security (pages 437 - 438) Wikipedia http://en.wikipedia.org/wiki/FIFO

QUESTION 215
Which of the following layers provides end-to-end data transfer service?

A. Network Layer.

B. Data Link Layer.

C. Transport Layer.

D. Presentation Layer.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: It is the Transport Layer that is responsible for reliable end-to-end data transfer between end systems.
The following answers are incorrect:
Network Layer. Is incorrect because the Network Layer is the OSI layer that is responsible for routing, switching, and subnetwork access across the entire OSI environment. Data Link Layer. Is incorrect because the Data Link Layer is the serial communications path between nodes or devices without any intermediate switching nodes. Presentation Layer. Is incorrect because the Presentation Layer is the OSI layer that determines how application information is represented (i.e., encoded) while in transit between two end systems.

QUESTION 216
The IP header contains a protocol field. If this field contains the value of 17, what type of data is contained within the ip datagram?

A. TCP.

B. ICMP.

C. UDP.

D. IGMP.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: If the protocol field has a value of 17 then it would indicate it was UDP.
The following answers are incorrect answers:

TCP. Is incorrect because the value for a TCP protocol would be 6. ICMP. Is incorrect because the value for an ICMP protocol would be 1. IGMP. Is incorrect because the value for an IGMP protocol would be 2. The protocol field of the IP packet dictates what protocol the IP packet is using.
TCP=6, ICMP=1, UDP=17, IGMP=2
Reference(s) used for this question:
SANS http://www.sans.org/resources/tcpip.pdf?ref=3871

QUESTION 217
How do you distinguish between a bridge and a router?

A. A bridge simply connects multiple networks, a router examines each packet to determine which network to forward it to.
B. "Bridge" and "router" are synonyms for equipment used to join two networks.
C. The bridge is a specific type of router used to connect a LAN to the global Internet.
D. The bridge connects multiple networks at the data link layer, while router connects multiple networks at the network layer.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: A bridge operates at the Data Link Layer and a router operates at the Network Layer.
The following answers are incorrect:
A bridge simply connects multiple networks, a router examines each packet to determine which network to forward it to. Is incorrect because both forward packets this is not distinctive enough. "Bridge" and "router" are synonyms for equipment used to join two networks. Is incorrect because the two are unique and operate at different layers of the OSI model. The bridge is a specific type of router used to connect a LAN to the global Internet. Is incorrect because a bridge does not connect a LAN to the global internet, but connects networks together creating a LAN.

QUESTION 218
ICMP and IGMP belong to which layer of the OSI model?

A. Datagram Layer.
B. Network Layer.
C. Transport Layer.
D. Data Link Layer.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The network layer contains the Internet Protocol (IP), the Internet Control Message Protocol (ICMP), and the Internet Group Management Protocol (IGMP) The following answers are incorrect:
Datagram Layer. Is incorrect as a distractor as there is no Datagram Layer. Transport Layer. Is incorrect because it is used to data between applications and uses the TCP and UDP protocols.
Data Link Layer. Is incorrect because this layer deals with addressing hardware.

QUESTION 219
Telnet and rlogin use which protocol?

A. UDP.
B. SNMP.
C. TCP.
D. IGP.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: TCP allows for reliabilty in connections which would be required for terminal emulation.
The following answers are incorrect:
UDP. Is incorrect because with User Datagram Protocol (UDP) you don't have a reliable transmission, datagrams could arrive out of sequence.
SNMP. Is incorrect because it is a network management protocol, Simple Network Management Protocol (SNMP).
IGP. Is incorrect because Interior Gateway Protocol (IGP) is used interally on a network.

QUESTION 220
What is a limitation of TCP Wrappers?

A. It cannot control access to running UDP services.
B. It stops packets before they reach the application layer, thus confusing some proxy servers.
C. The hosts. access control system requires a complicated directory tree.
D. They are too expensive.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: TCP Wrappers can control when a UDP server starts but has little control afterwards because UDP packets can be sent randomly.
The following answers are incorrect:
It stops packets before they reach the application layer, thus confusing some proxy servers. Is incorrect because the TCP Wrapper acts as an ACL restricting packets so would not confuse a proxy server because the packets would not arrive and would not be a limitation. The hosts. access control system requires a complicated directory tree. Is incorrect because a simple directory tree is involved.
They are too expensive. Is incorrect because TCP Wrapper is considered open source with a BSD licensing scheme.

QUESTION 221
The IP header contains a protocol field. If this field contains the value of 6, what type of data is contained within the ip datagram?

A. TCP.
B. ICMP.
C. UDP.
D. IGMP.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: If the protocol field has a value of 6 then it would indicate it was TCP. The protocol field of the IP packet dictates what protocol the IP packet is using.
TCP=6, ICMP=1, UDP=17, IGMP=2
The following answers are incorrect:
ICMP. Is incorrect because the value for an ICMP protocol would be 1. UDP. Is incorrect because the value for an UDP protocol would be 17. IGMP. Is incorrect because the value for an IGMP protocol would be 2.

SANS http://www.sans.org/resources/tcpip.pdf?ref=3871

QUESTION 222

The IP header contains a protocol field. If this field contains the value of 1, what type of data is contained within the IP datagram?

A. TCP.
B. ICMP.
C. UDP.
D. IGMP.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: If the protocol field has a value of 1 then it would indicate it was ICMP.
The following answers are incorrect:
TCP. Is incorrect because the value for a TCP protocol would be 6. UDP. Is incorrect because the value for an UDP protocol would be 17. IGMP. Is incorrect because the value for an IGMP protocol would be 2.

QUESTION 223
The IP header contains a protocol field. If this field contains the value of 2, what type of data is contained within the IP datagram?

A. TCP.
B. ICMP.
C. UDP.
D. IGMP.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: If the protocol field has a value of 2 then it would indicate it was IGMP. The following answers are incorrect:
TCP. Is incorrect because the value for a TCP protocol would be 6. UDP. Is incorrect because the value for an UDP protocol would be 17. ICMP. Is incorrect because the value for an ICMP protocol would be 1.

QUESTION 224
What is the proper term to refer to a single unit of Ethernet data at the link layer of the DoD TCP model ?

A. Ethernet Segment.
B. Ethernet Datagram.
C. Ethernet Frame.
D. Ethernet Packet.

Correct Answer: C
Explanation

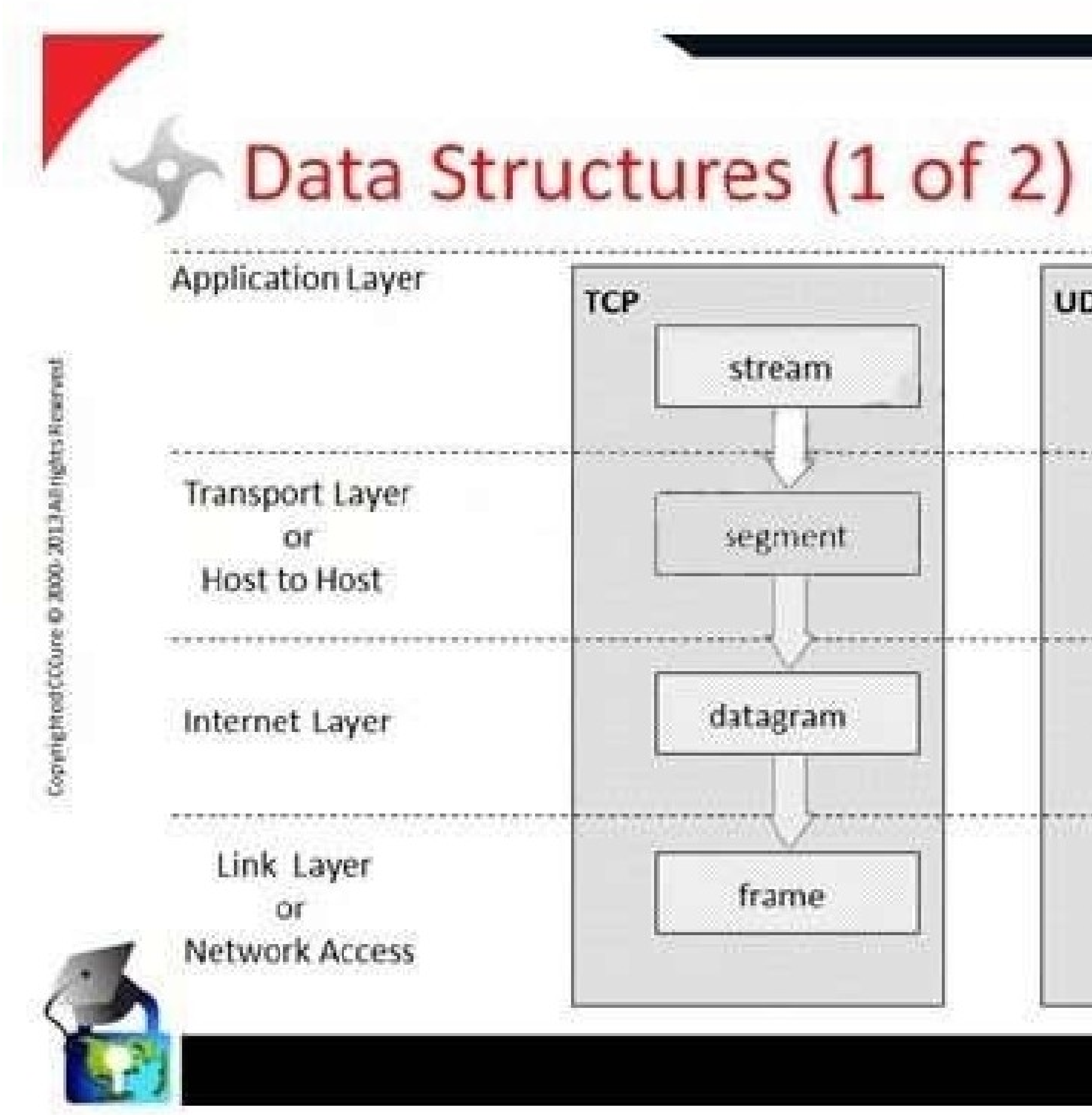
Explanation/Reference:
Explanation: Ethernet is frame based network technology.
See below a few definitions from RFC 1122:
SEGMENT
A segment is the unit of end-to-end transmission in the TCP protocol. A segment consists of a TCP header followed by application data. A segment is transmitted by encapsulation inside an IP datagram.
PACKET
A packet is the unit of data passed across the interface between the internet layer and the link layer. It includes an IP header and data. A packet may be a complete IP datagram or a fragment of an IP datagram.
FRAME

A frame is the unit of transmission in a link layer protocol, and consists of a link-layer header followed by a packet.

The following answers are incorrect:

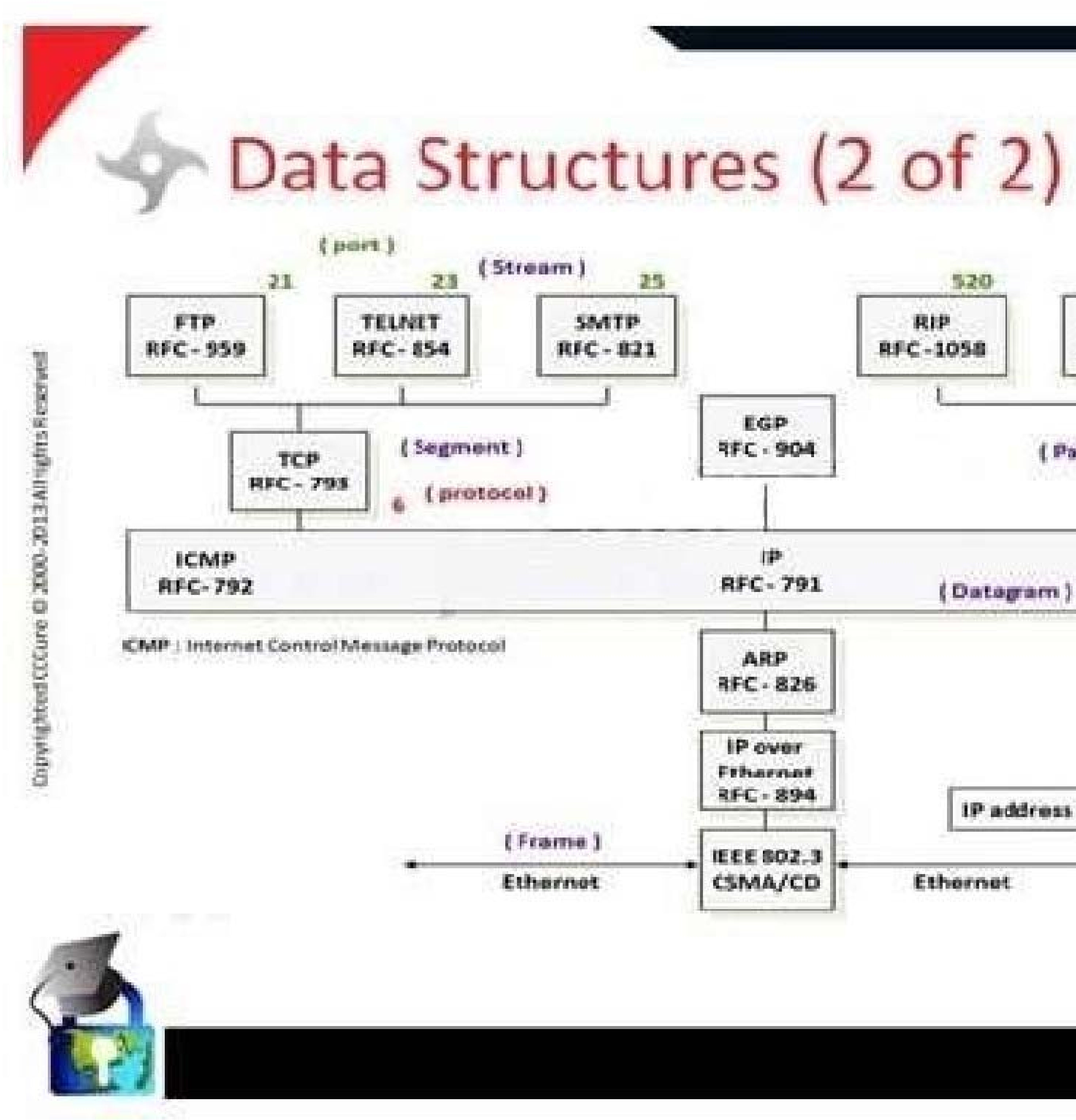
Ethernet segment. Is incorrect because Ethernet segment is a distractor, TCP segment would be the correct terminology. Ethernet is a frame based network technology, Ethernet datagram. Is incorrect because Ethernet datagram is a distractor, IP datagram would be the correct terminology. Ethernet is a frame based network technology Ethernet packet. Is incorrect because Ethernet packet is a distractor, a Packet is a group of information so would not be a "single unit". Ethernet is a frame based network technology. Look at the diagrams below that were extracted from my Security+ Computer Based Tutorial.

TCP/IP Data Structures



Data Structures (1 of 2)

IMPORTANT NOTE:
The names used on the diagram above are from RFC 1122 which describe the DOD Model. Vendors and Books may use slightly different names or even number of layers.



Data Structures (2 of 2)

(port)

(Stream)

21

23

25

520

FTP
RFC - 959

TELNET
RFC - 854

SMTP
RFC - 821

RIP
RFC -1058

EGP
RFC - 904

TCP
RFC - 793

(Segment)

6 (protocol)

(Pa

ICMP
RFC- 792

IP
RFC - 791

(Datagram)

ICMP : Internet Control Message Protocol

ARP
RFC - 826

IP over
Ethernet
RFC - 894

IP address

(Frame)

Ethernet

IEEE 802.3
CSMA/CD

Ethernet

Copyrighted CCure © 2000-2013 All rights Reserved

TCP/IP Data Structure
The following Reference(s) were used for this question:
Wikipedia http://en.wikipedia.org/wiki/Ethernet

QUESTION 225
What is the proper term to refer to a single unit of IP data?

A. IP segment.

B. IP datagram.

C. IP frame.

D. IP fragment.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: IP is a datagram based technology.
DIFFERENCE BETWEEN PACKETS AND DATAGRAM
As specified at: http://en.wikipedia.org/wiki/Packet_(information_technology) In general, the term packet applies to any message formatted as a packet, while the term datagram is generally reserved for packets of an "unreliable" service. A "reliable" service is one that notifies the user if delivery fails, while an "unreliable" one does not notify the user if delivery fails. For example, IP provides an unreliable service. Together, TCP and IP provide a reliable service, whereas UDP and IP provide an unreliable one. All these protocols use packets, but UDP packets are generally called datagrams. If a network does not guarantee packet delivery, then it becomes the host's responsibility to provide reliability by detecting and retransmitting lost packets. Subsequent experience on the ARPANET indicated that the network itself could not reliably detect all packet delivery failures, and this pushed responsibility for error detection onto the sending host in any case. This led to the development of the end-to-end principle, which is one of the Internet's fundamental design assumptions.
The following answers are incorrect:
IP segment. Is incorrect because IP segment is a detractor, the correct terminology is TCP segment. IP is a datagram based technology.
IP frame. Is incorrect because IP frame is a detractor, the correct terminology is Ethernet frame. IP is a datagram based technology.
IP fragment. Is incorrect because IP fragment is a detractor.

Wikipedia http://en.wikipedia.org/wiki/Internet_Protocol

QUESTION 226
You are running a packet sniffer on a network and see a packet containing a long string of "0x90 0x90 0x90 0x90...." in the middle of it traveling to an x86-based machine as a target. This could be indicative of what activity being attempted?

A. Over-subscription of the traffic on a backbone.

B. A source quench packet.

C. A FIN scan.

D. A buffer overflow attack.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: A series of the same control characters, hexadecimal code, imbedded in the string is usually an indicator of a buffer overflow attack.
The Intel x86 processors use the hexadecimal number 90 to represent NOP (no operation). Many buffer overflow attacks use long strings of control characters and this is representative of that type of attack.
A buffer overflow takes place when too much data are accepted as input to a specific process. A buffer is an allocated segment of memory. A buffer can be overflowed arbitrarily with too much data, but for it to be of any use to an attacker, the code inserted into the buffer must be of a specific length, followed up by commands the attacker wants executed. So, the purpose of a buffer overflow may be either to make a mess, by shoving arbitrary data into various memory segments, or to accomplish a specific task, by pushing into the memory segment a carefully crafted set of data that will accomplish a specific task. This task could be to open a command shell with administrative privilege or execute malicious code.
Common threats to system availability, integrity, and confidentiality include hardware failure, misuse of system

privileges, buffer overflows and other memory attacks, denial of service, reverse engineering, and system hacking.
Since many vulnerabilities result from insecure design and most threats are well known, it is the responsibility of the security architect to ensure that their designs are addressing security requirements appropriately while also ensuring that the system can continue to perform its intended function.
The following answers are incorrect:
Over-subscription of the traffic on a backbone. Is incorrect because if there was Over-subscription of the traffic on a backbone, that would typically result in not being able to send or receive any packets, more commonly known as Denial of Service or DoS. A source quench packet. This is incorrect because a source quench packet is an ICMP message that contains the internet header plus 64 bits of the original datagram. A FIN scan. This is incorrect because a FIN scan is when a packet with the FIN flag set is sent to a specific port and the results are then analyzed.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition, Security Architecture and Design, Page 332, for people using the Kindle edition you will find it at Kindle Locations 7310- 7315.
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Security Architecture and Design (Kindle Locations 1403-1407). . Kindle Edition.
Wikipedia http://en.wikipedia.org/wiki/Port_scanner
ICMP http://security.maruhn.com/iptables-tutorial/x1078.html Wikipedia http://en.wikipedia.org/wiki/Buffer_overflow

QUESTION 227
A packet containing a long string of NOP's followed by a command is usually indicative of what?

A. A syn scan.
B. A half-port scan.
C. A buffer overflow attack.
D. A packet destined for the network's broadcast address.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: A series of the same control, hexidecimal, characters imbedded in the string is usually an indicator of a buffer overflow attack. A NOP is a instruction which does nothing (No Operation - the hexadecimal equivalent is 0x90)
The following answers are incorrect:
A syn scan. This is incorrect because a SYN scan is when a SYN packet is sent to a specific port and the results are then analyzed.
A half-port scan. This is incorrect because the port scanner generates a SYN packet. If the target port is open, it will respond with a SYN-ACK packet. The scanner host responds with a RST packet, closing the connection before the handshake is completed. Also known as a Half Open Port scan.
A packet destined for the network's broadcast address. This is incorrect because this type of packet would not contain a long string of NOP characters.

QUESTION 228
In the days before CIDR (Classless Internet Domain Routing), networks were commonly organized by classes. Which of the following would have been true of a Class B network?

A. The first bit of the IP address would be set to zero.
B. The first bit of the IP address would be set to one and the second bit set to zero.
C. The first two bits of the IP address would be set to one, and the third bit set to zero.
D. The first three bits of the IP address would be set to one.

Correct Answer: C
Explanation

Explanation/Reference:

Explanation: Each Class B network address has a 16-bit network prefix, with the two highest order bits set to 1-0.

The following answers are incorrect:

The first bit of the IP address would be set to zero. Is incorrect because, this would be a Class A network address.

The first two bits of the IP address would be set to one, and the third bit set to zero. Is incorrect because, this would be a Class C network address.

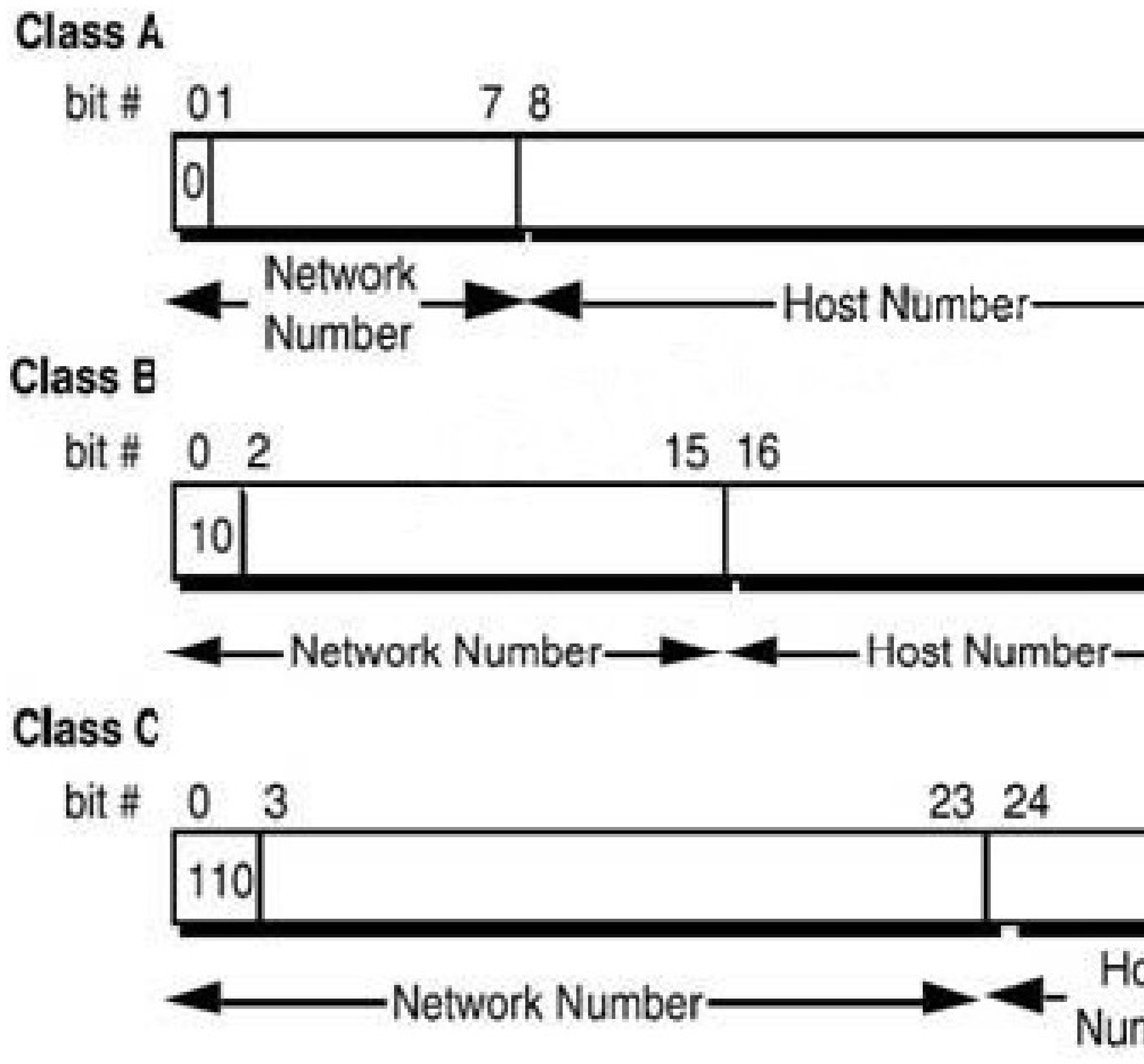
The first three bits of the IP address would be set to one. Is incorrect because, this is a distractor. Class D & E have the first three bits set to 1. Class D the 4th bit is 0 and for Class E the 4th bit to 1.

Classless Internet Domain Routing (CIDR)

High Order bits are shown in bold below.

For Class A, the addresses are 0.0.0.0 - 127.255.255.255 The lowest Class A address is represented in binary as 00000000.00000000.0000000.00000000 For Class B networks, the addresses are 128.0.0.0 - 191.255.255.255. The lowest Class B address is represented in binary as 10000000.00000000.00000000.00000000 For Class C, the addresses are 192.0.0.0 - 223.255.255.255 The lowest Class C address is represented in binary as 11000000.00000000.00000000.00000000 For Class D, the addresses are 224.0.0.0 - 239.255.255.255 (Multicast) The lowest Class D address is represented in binary as 11100000.00000000.00000000.00000000 For Class E, the addresses are 240.0.0.0 - 255.255.255.255 (Reserved for future usage) The lowest Class E address is represented in binary as 11110000.00000000.00000000.00000000 Classful IP Address Format

FIGURE 4. Principle Classful IP Address Form



3Com http://www.3com.com/other/pdfs/infra/corpinfo/en_US/501302.pdf AIOv3 Telecommunications and Networking Security (page 438)

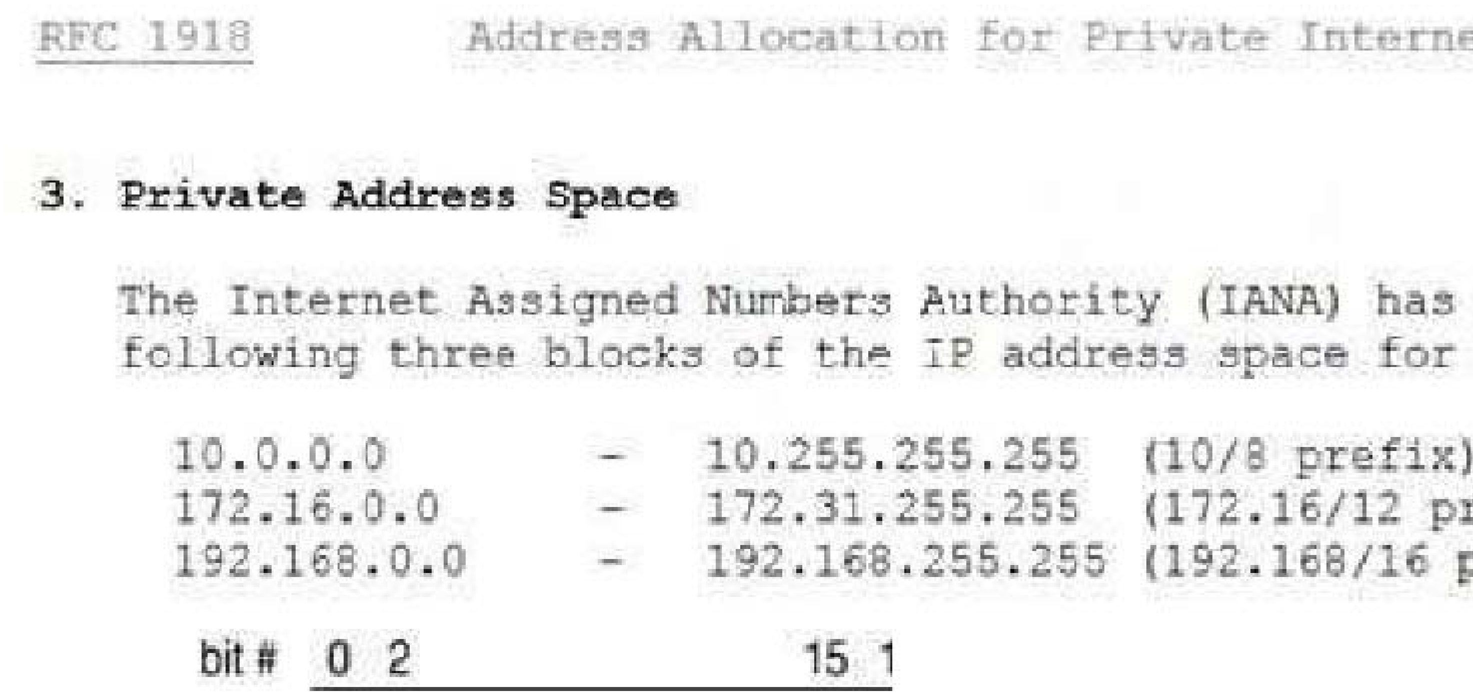
QUESTION 229
Which of the following is an IP address that is private (i.e. reserved for internal networks, and not a valid address to use on the Internet)?

A. 192.168.42.5

B. 192.166.42.5
C. 192.175.42.5
D. 192.1.42.5

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: This is a valid Class C reserved address. For Class C, the reserved addresses are 192.168.0.0 - 192.168.255.255.
The private IP address ranges are defined within RFC 1918:
RFC 1918 private ip address range



```
RFC 1918        Address Allocation for Private Interne

3. Private Address Space

   The Internet Assigned Numbers Authority (IANA) has
   following three blocks of the IP address space for

     10.0.0.0        -   10.255.255.255  (10/8 prefix)
     172.16.0.0      -   172.31.255.255  (172.16/12 pr
     192.168.0.0     -   192.168.255.255 (192.168/16 p

      bit #  0  2               15  1
```

The following answers are incorrect:
192.166.42.5 Is incorrect because it is not a Class C reserved address. 192.175.42.5 Is incorrect because it is not a Class C reserved address. 192.1.42.5 Is incorrect because it is not a Class C reserved address.

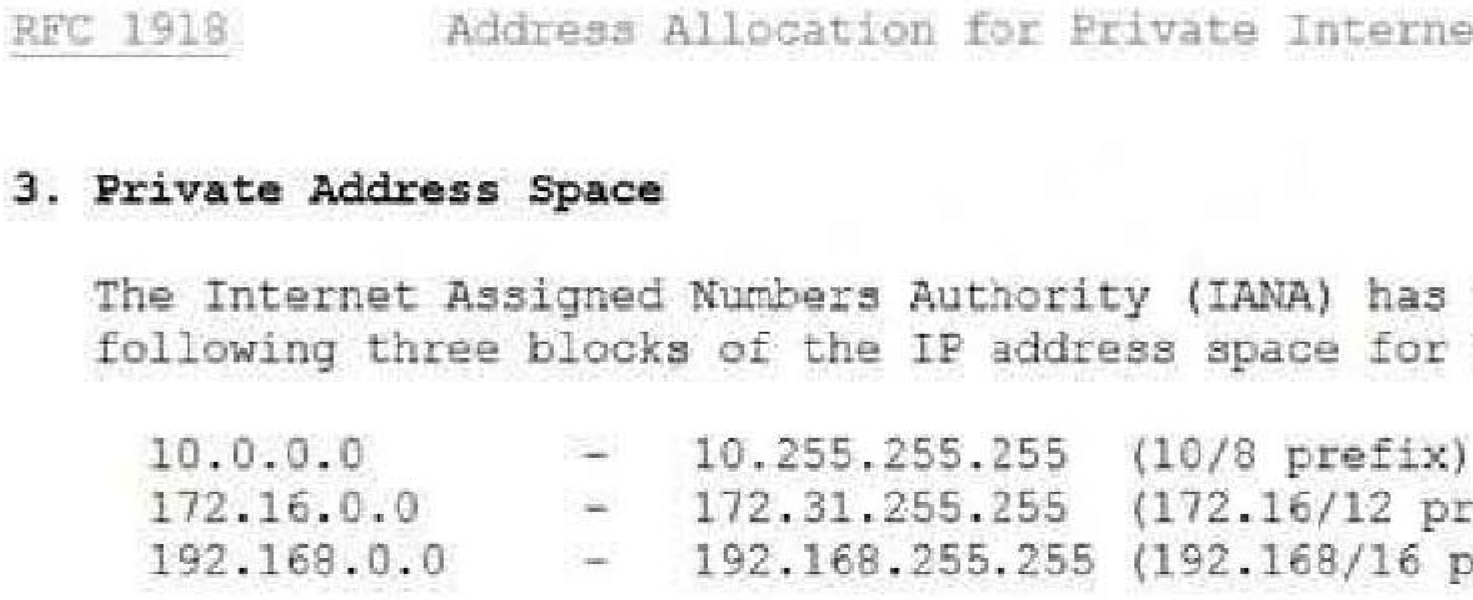
QUESTION 230
Which of the following is an IP address that is private (i.e. reserved for internal networks, and not a valid address to use on the Internet)?

A. 172.12.42.5
B. 172.140.42.5
C. 172.31.42.5
D. 172.15.42.5

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: This is a valid Class B reserved address. For Class B networks, the reserved addresses are 172.16.0.0 - 172.31.255.255.
The private IP address ranges are defined within RFC 1918:

RFC 1918 private ip address range



```
RFC 1918          Address Allocation for Private Interne

3. Private Address Space

   The Internet Assigned Numbers Authority (IANA) has
   following three blocks of the IP address space for

     10.0.0.0        -   10.255.255.255  (10/8 prefix)
     172.16.0.0      -   172.31.255.255  (172.16/12 pr
     192.168.0.0     -   192.168.255.255 (192.168/16 p
```

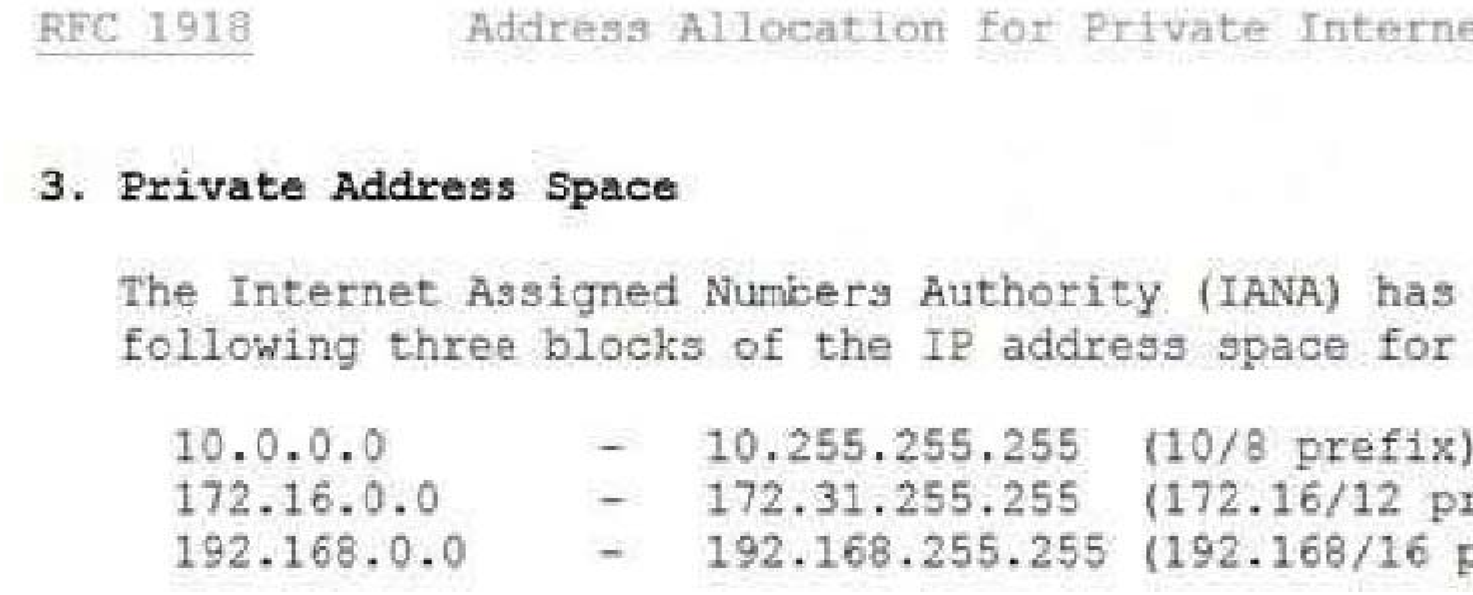
The following answers are incorrect:
172.12.42.5 Is incorrect because it is not a Class B reserved address. 172.140.42.5 Is incorrect because it is not a Class B reserved address. 172.15.42.5 Is incorrect because it is not a Class B reserved address.

QUESTION 231
Which of the following is an IP address that is private (i.e. reserved for internal networks, and not a valid address to use on the Internet)?

A. 10.0.42.5
B. 11.0.42.5
C. 12.0.42.5
D. 13.0.42.5

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: This is a valid Class A reserved address. For Class A, the reserved addresses are 10.0.0.0 - 10.255.255.255.
The following answers are incorrect:
11.0.42.5 Is incorrect because it is not a Class A reserved address. 12.0.42.5 Is incorrect because it is not a Class A reserved address. 13.0.42.5 Is incorrect because it is not a Class A reserved address. The private IP address ranges are defined within RFC 1918:
RFC 1918 private ip address range



```
RFC 1918        Address Allocation for Private Interne

3. Private Address Space

   The Internet Assigned Numbers Authority (IANA) has
   following three blocks of the IP address space for

     10.0.0.0        -   10.255.255.255  (10/8 prefix)
     172.16.0.0      -   172.31.255.255  (172.16/12 pr
     192.168.0.0     -   192.168.255.255 (192.168/16 p
```

3Com http://www.3com.com/other/pdfs/infra/corpinfo/en_US/501302.pdf AIOv3 Telecommunications and Networking Security (page 438)

QUESTION 232
Which of the following media is MOST resistant to tapping?

A. microwave.
B. twisted pair.
C. coaxial cable.
D. fiber optic.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Fiber Optic is the most resistant to tapping because Fiber Optic uses a light to transmit the signal. While there are some technologies that will allow to monitor the line passively, it is very difficult to tap into without detection sot this technology would be the MOST resistent to tapping.
The following answers are in correct:
microwave. Is incorrect because microwave transmissions can be intercepted if in the path of the broadcast without detection.
twisted pair. Is incorrect because it is easy to tap into a twisted pair line. coaxial cable. Is incorrect because it is easy to tap into a coaxial cable line.

QUESTION 233
Which of the following is a tool often used to reduce the risk to a local area network (LAN) that has external connections by filtering Ingress and Egress traffic?

A. a firewall.
B. dial-up.
C. passwords.
D. fiber optics.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The use of a firewall is a requirement to protect a local area network (LAN) that has external connections without that you have no real protection from fraudsters.
The following answers are incorrect:
dial-up. This is incorrect because this offers little protection once the connection has been established.
passwords. This is incorrect because there are tools to crack passwords and once a user has been authenticated and connects to the external connections, passwords do not offer protection against incoming TCP packets.
fiber optics. This is incorrect because this offers no protection from the external connection.

QUESTION 234
Which of the following protocols suite does the Internet use?

A. IP/UDP/TCP
B. IP/UDP/ICMP/TCP
C. TCP/IP
D. IMAP/SMTP/POP3

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Transmission Control Protocol/Internet Protocol (TCP/IP) is the common name for the suite of protocols that was developed by the Department of Defense (DoD) in the 1970's to support the construction of the internet. The Internet is based on TCP/IP. The Internet protocol suite is the networking model and a set of communications protocols used for the Internet and similar networks. It is commonly known as TCP/IP, because its most important protocols, the Transmission Control Protocol (TCP) and the Internet Protocol (IP), were the first networking protocols defined in this standard. It is occasionally known as the DoD model, because the development of the networking model was funded by DARPA, an agency of the United States Department of Defense.
TCP/IP provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. This functionality has been organized into four abstraction layers within the DoD Model which are used to sort all related protocols according to the scope of networking involved.
From lowest to highest, the layers are:
The link layer, containing communication technologies for a single network segment (link), The internet layer, connecting independent networks, thus establishing internetworking, The transport layer handling process-to-process communication, The application layer, which interfaces to the user and provides support services. The TCP/IP model and related protocols are maintained by the Internet Engineering Task Force (IETF).
The following answers are incorrect:
IP/UDP/TCP. This is incorrect, all three are popular protocol and they are not considered a suite of protocols.
IP/UDP/ICMP/TCP. This is incorrect, all 4 are some of the MOST commonly used protocol but they are not called a suite of protocol.
IMAP/SMTP/POP3 . This is incorrect because they are all email protocol and consist of only a few of the protocol that would be included in the TCP/IP suite of protocol.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 5267-5268). Auerbach Publications. Kindle Edition.
http://en.wikipedia.org/wiki/Internet_protocol_suite

QUESTION 235
Organizations should consider which of the following first before allowing external access to their LANs via the Internet?

A. plan for implementing workstation locking mechanisms.
B. plan for protecting the modem pool.
C. plan for providing the user with his account usage information.

D. plan for considering proper authentication options.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Before a LAN is connected to the Internet, you need to determine what the access controls mechanisms are to be used, this would include how you are going to authenticate individuals that may access your network externally through access control.
The following answers are incorrect:
plan for implementing workstation locking mechanisms. This is incorrect because locking the workstations have no impact on the LAN or Internet access. plan for protecting the modem pool. This is incorrect because protecting the modem pool has no impact on the LAN or Internet access, it just protects the modem. plan for providing the user with his account usage information. This is incorrect because the question asks what should be done first. While important your primary concern should be focused on security.

QUESTION 236
Which one of the following is usually not a benefit resulting from the use of firewalls?

A. reduces the risks of external threats from malicious hackers.
B. prevents the spread of viruses.
C. reduces the threat level on internal system.
D. allows centralized management and control of services.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: This is not a benefit of a firewall. Most firewalls are limited when it comes to preventing the spread of viruses.
This question is testing your knowledge of Malware and Firewalls. The keywords within the questions are "usually" and "virus". Once again to come up with the correct answer, you must stay within the context of the question and really ask yourself which of the 4 choices is NOT usually done by a firewall.
Some of the latest Appliances such as Unified Threat Management (UTM) devices does have the ability to do virus scanning but most first and second generation firewalls would not have such ability. Remember, the questions is not asking about all possible scenarios that could exist but only about which of the 4 choices presented is the BEST. For the exam you must know your general classes of Malware. There are generally four major classes of malicious code that fall under the general definition of malware:
1. Virus: Parasitic code that requires human action or insertion, or which attaches itself to another program to facilitate replication and distribution. Virus-infected containers can range from e-mail, documents, and data file macros to boot sectors, partitions, and memory fobs. Viruses were the first iteration of malware and were typically transferred by floppy disks (also known as "sneakernet") and injected into memory when the disk was accessed or infected files were transferred from system to system.
2. Worm: Self-propagating code that exploits system or application vulnerabilities to replicate. Once on a system, it may execute embedded routines to alter, destroy, or monitor the system on which it is running, then move on to the next system. A worm is effectively a virus that does not require human interaction or other programs to infect systems.
3. Trojan Horse: Named after the Trojan horse of Greek mythology (and serving a very similar function), a Trojan horse is a general term referring to programs that appear desirable, but actually contain something harmful. A Trojan horse purports to do one thing that the user wants while secretly performing other potentially malicious actions. For example, a user may download a game file, install it, and begin playing the game. Unbeknownst to the user, the application may also install a virus, launch a worm, or install a utility allowing an attacker to gain unauthorized access to the system remotely, all without the user's knowledge.
4. Spyware: Prior to its use in malicious activity, spyware was typically a hidden application injected through poor browser security by companies seeking to gain more information about a user's Internet activity. Today, those methods are used to deploy other malware, collect private data, send advertising or commercial messages to a system, or monitor system input, such as keystrokes or mouse clicks.
The following answers are incorrect:

reduces the risks of external threats from malicious hackers. This is incorrect because a firewall can reduce the risks of external threats from malicious hackers. reduces the threat level on internal system. This is incorrect because a firewall can reduce the threat level on internal system.
allows centralized management and control of services. This is incorrect because a firewall can allow centralize management and control of services.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 3989-4009). Auerbach Publications. Kindle Edition.

QUESTION 237
Which of the following OSI layers provides routing and related services?

A. Network Layer
B. Presentation Layer
C. Session Layer
D. Physical Layer

Correct Answer: A
Explanation

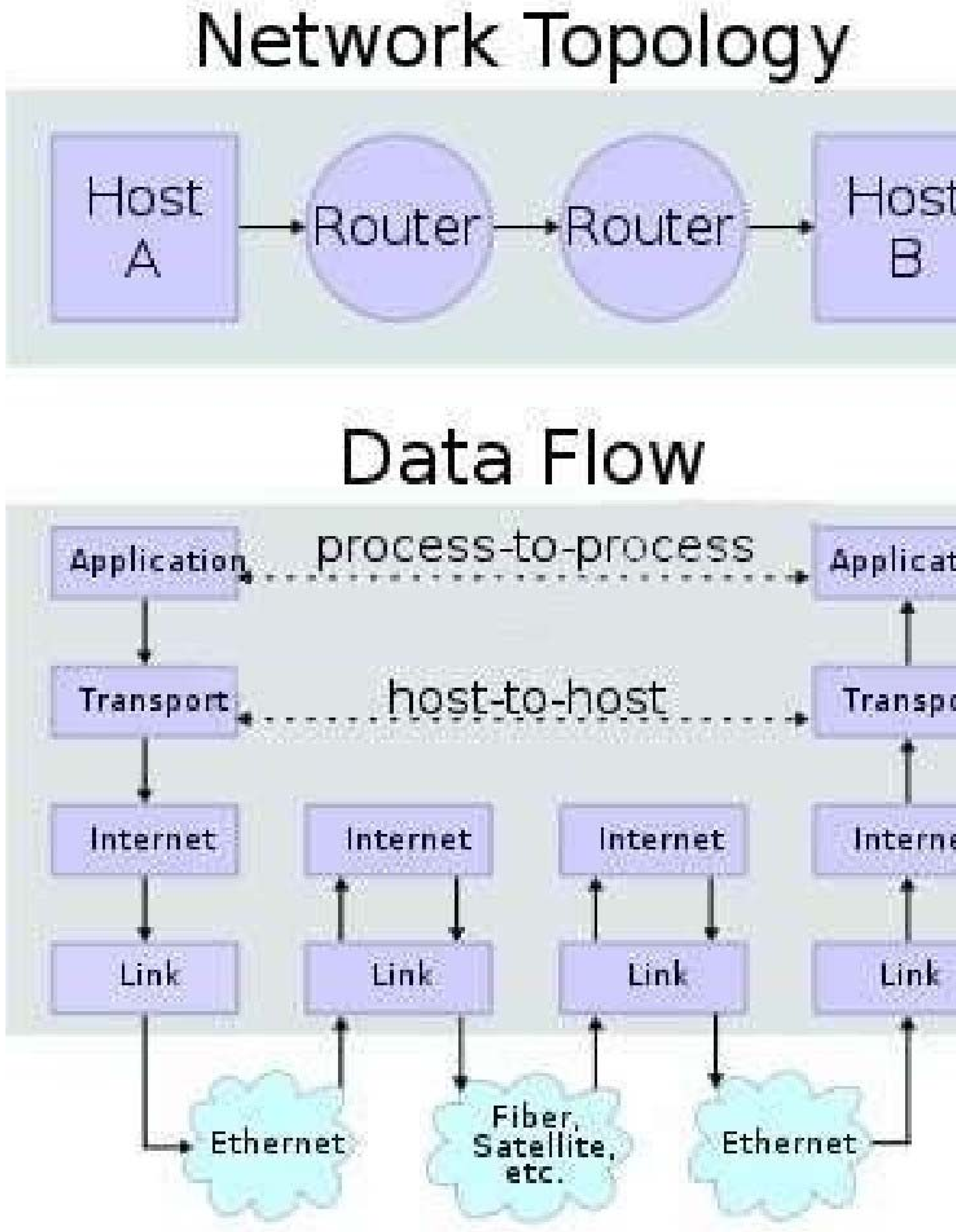
Explanation/Reference:
Explanation: The Network Layer performs network routing functions.
The following answers are incorrect:
Presentation Layer. Is incorrect because the Presentation Layer transforms the data to provide a standard interface for the Application layer.
Session Layer. Is incorrect because the Session Layer controls the dialogues/connections (sessions) between computers.
Physical Layer. is incorrect because the Physical Layer defines all the electrical and physical specifications for devices.

QUESTION 238
Which of the following DoD Model layer provides non-repudiation services?

A. network layer.
B. application layer.
C. transport layer.
D. data link layer.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The Application Layer determines the identity of the communication partners and this is where Non-Repudiation service would be provided as well. See the layers below:


Network Topology
Host A
Router
Router
Host B
Data Flow
process-to-process
host-to-host
Application
Transport
Internet
Link
Internet
Link
Internet
Link
Application
Transport
Internet
Link
Ethernet
Fiber, Satellite, etc.
Ethernet

DOD Model DoD Model
The following answers are incorrect:
network layer. Is incorrect because the Network Layer mostly has routing protocols, ICMP, IP, and IPSEC. It it not a layer in the DoD Model. It is called the Internet Layer within the DoD model. transport layer. Is incorrect because the Transport layer provides transparent transfer of data between end users. This is called Host-to-Host on the DoD model but sometimes some books will call it Transport as well on the DoD model.
data link layer. Is incorrect because the Data Link Layer defines the protocols that computers must follow to access the network for transmitting and receiving messages. It is part of the OSI Model. This does not exist on the DoD model, it is called the Link Layer on the DoD model.

QUESTION 239
What is the 802.11 standard related to?

A. Public Key Infrastructure (PKI)
B. Wireless network communications
C. Packet-switching technology
D. The OSI/ISO model

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The 802.11 standard outlines how wireless clients and APs communicate, lays out the specifications of their interfaces, dictates how signal transmission should take place, and describes how authentication, association, and security should be implemeted.
The following answers are incorrect:
Public Key Infrastructure (PKI) Public Key Infrastructure is a supporting infrastructure to manage public keys. It is not part of the IEEE 802 Working Group standard. Packet-switching technology A packet-switching technology is not included in the IEEE 802 Working Group standard. It is a technology where-in messages are broken up into packets, which then travel along different routes to the destination. The OSI/ISO model The Open System Interconnect model is a sevel-layer model defined as an international standard describing network communications. The following reference(s) were/was used to create this question:
Source: Shon Harris - "All-in-One CISSP Exam Guide" Fourth Edition; Chapter 7 - Telecommunications and Network Security: pg. 624.
802.11 refers to a family of specifications developed by the IEEE for Wireless LAN technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. The IEEE accepted the specification in 1997. There are several specifications in the 802.11 family:
802.11 # applies to wireless LANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).
802.11a # an extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 5GHz band. 802.11a uses an orthogonal frequency division multiplexing encoding scheme rather than FHSS or DSSS. 802.11b (also referred to as 802.11 High Rate or Wi-Fi) # an extension to 802.11 that applies to wireless LANS and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. 802.11b was a 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet. 802.11g # applies to wireless LANs and provides 20+ Mbps in the 2.4 GHz band. Source: 802.11 Planet's web site.

QUESTION 240
Remote Procedure Call (RPC) is a protocol that one program can use to request a service from a program located in another computer in a network. Within which OSI/ISO layer is RPC implemented?

A. Session layer
B. Transport layer
C. Data link layer
D. Network layer

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The
Answer: Session layer, which establishes, maintains and manages sessions and synchronization of data flow. Session layer protocols control application-to-application communications, which is what an RPC call is.
The following answers are incorrect:
Transport layer: The Transport layer handles computer-to computer communications, rather than application-to-application communications like RPC.
Data link Layer: The Data Link layer protocols can be divided into either Logical Link Control (LLC) or Media Access Control (MAC) sublayers. Protocols like SLIP, PPP, RARP and L2TP are at this layer. An application-to-application protocol like RPC would not be addressed at this layer. Network layer: The Network Layer is mostly concerned with routing and addressing of information, not application-to-application communication calls such as an RPC call. The following reference(s) were/was used to create this question:
The Remote Procedure Call (RPC) protocol is implemented at the Session layer, which establishes, maintains and manages sessions as well as synchronization of the data flow.
Source: Jason Robinett's CISSP Cram Sheet: domain2.
Source: Shon Harris AIO v3 pg. 423

QUESTION 241
Within the OSI model, at what layer are some of the SLIP, CSLIP, PPP control functions provided?

A. Data Link
B. Transport
C. Presentation
D. Application

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: RFC 1661 - The Point-to-Point Protocol (PPP) specifies that the Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams over pointto- point links. PPP is comprised of three main components:
1 A method for encapsulating multi-protocol datagrams. 2 A Link Control Protocol (LCP) for establishing, configuring, and testing the data-link connection. 3 A family of Network Control Protocols (NCPs) for establishing and configuring different networklayer protocols.

QUESTION 242
In the Open Systems Interconnect (OSI) Reference Model, at what level are TCP and UDP provided?

A. Transport
B. Network
C. Presentation
D. Application

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The
Answer: Transport. The Layer 4 Transport layer supports the TCP and UDP protocols in the OSI Reference Model. This layer creates an end-to-end transportation between peer hosts. The transmission can be connectionless and unreliable such as UDP, or connectionoriented and ensure error-free delivery such as TCP.
The following answers are incorrect:

Network. The Network layer moves information between hosts that are not physically connected. It deals with routing of information. IP is a protocol that is used in Network Layer. TCP and UDP do not reside at the Layer 3 Network Layer in the OSI Reference Model. Presentation. The Presentation Layer is concerned with the formatting of data into a standard presentation such as
ASCII. TCP and UDP do not reside at the Layer 6 Presentation Layer in the OSI Reference Model. Application. The Application Layer is a service for applications and Operating Systems data transmission, for example HTTP, FTP and SMTP. TCP and UDP do not reside at the Layer 7 Application Layer in the OSI Reference Model.
The following reference(s) were/was used to create this question:
ISC2 OIG, 2007 p. 411
Shon Harris AIO v.3 p. 424

QUESTION 243
FTP, TFTP, SNMP, and SMTP are provided at what level of the Open Systems Interconnect (OSI) Reference Model?

A. Application
B. Network
C. Presentation
D. Transport

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The
Answer: Application. The Layer 7 Application Layer of the Open Systems Interconnect (OSI) Reference Model is a service for applications and Operating Systems data transmission, for example FTP, TFTP, SNMP, and SMTP.
The following answers are incorrect:
Network. The Network layer moves information between hosts that are not physically connected. It deals with routing of information. IP is a protocol that is used in Network Layer. FTP, TFTP, SNMP, and SMTP do not reside at the Layer 3 Network Layer in the OSI Reference Model. Presentation. The Presentation Layer is concerned with the formatting of data into a standard presentation such as
ASCII. FTP, TFTP, SNMP, and SMTP do not reside at the Layer 6 Presentation Layer in the OSI Reference Model.
Transport. The Transport Layer creates an end-to-end transportation between peer hosts. The transmission can be connectionless and unreliable such as UDP, or connection-oriented and ensure error-free delivery such as TCP. FTP, TFTP, SNMP, and SMTP do not reside at the Layer 4 Transportation Layer in the OSI Reference Model.
The following reference(s) were/was used to create this question: OSI/ISO.
Shon Harris AIO v.3 p. 420-421
ISC2 OIG, 2997 p.412-413

QUESTION 244
Which of the following is TRUE regarding Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)?

A. TCP is connection-oriented, UDP is not.
B. UDP provides for Error Correction, TCP does not.
C. UDP is useful for longer messages, rather than TCP.
D. TCP does not guarantee delivery of data, while UDP does guarantee data delivery.

Correct Answer: A
Explanation

Explanation/Reference:

Explanation: TCP is a reliable connection-oriented transport for guaranteed delivery of data. Protocols represent certain rules and regulations that are essential in order to have data communication between two entities. Internet Protocols work in sending and receiving data packets. This type of communication may be either connection-less or connection-oriented. In a connection-oriented scenario, an acknowledgement is being received by the sender from the receiver in support of a perfect transfer. Transmission Control Protocol or TCP is such a protocol. On the other hand, UDP or User Datagram Protocol is of the connection-less type where no feedback is being forwarded to the sender after delivery and the data transfer have taken place or not. Though, it's not a guaranteed method, but, once a connection is established, UDP works much faster than TCP as TCP has to rely on a feedback and accordingly, the entire 3-way handshaking takes place.
The following answers are incorrect:
UDP provides for Error Correction, TCP does not: UDP does not provide for error correction, while TCP does.
UDP is useful for longer messages, rather than TCP: UDP is useful for shorter messages due to its connectionless nature.
TCP does not guarantee delivery of data, while UDP does guarantee data delivery: The opposite is true.
References Used for this question:
http://www.cyberciti.biz/faq/key-differences-between-tcp-and-udp-protocols/ http://www.skullbox.net/tcpudp.php
James's TCP-IP FAQ - Understanding Port Numbers.

QUESTION 245
Which OSI/ISO layer is responsible for determining the best route for data to be transferred?

A. Session layer
B. Physical layer
C. Network layer
D. Transport layer

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The main responsibility of the network layer is to insert information into the packet's header so that it can be properly routed. The protocols at the network layer must determine the best path for the packet to take.
The following answers are incorrect:
Session layer. The session layer is responsible for establishing a connection between two applications.
Physical layer. The physical layer if responsible for converting electronic impulses into bits and vice-versa.
Transport layer. The transport layer is responsible for data transmission and error detection. The following reference(s) were/was used to create this question:
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, v3, chapter 7: Telecommunications and Network Security (page 422-428). ISC2 Official ISC2 Guide to the CBK (OIG) 2007, p. 409-412

QUESTION 246
Which of the following is true related to network sniffing?

A. Sniffers allow an attacker to monitor data passing across a network.
B. Sniffers alter the source address of a computer to disguise and exploit weak authentication methods.
C. Sniffers take over network connections.
D. Sniffers send IP fragments to a system that overlap with each other.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The following answers are incorrect: Sniffers alter the source address of a computer to disguise and exploit weak authentication methods. IP Spoofing is a network-based attack, which involves altering the

source address of a computer to disguise the attacker and exploit weak authentication methods.
Sniffers take over network connections. Session Hijacking tools allow an attacker to take over network connections, kicking off the legitimate user or sharing a login. Sniffers send IP fragments to a system that overlap with each other. Malformed Packet attacks are a type of DoS attack that involves one or two packets that are formatted in an unexpected way. Many vendor product implementations do not take into account all variations of user entries or packet types. If software handles such errors poorly, the system may crash when it receives such packets. A classic example of this type of attack involves sending IP fragments to a system that overlap with each other (the fragment offset values are incorrectly set. Some unpatched Windows and Linux systems will crash when the encounter such packets. The following reference(s) were/was used to create this question:
Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, Auerbach, NY, NY 2001, Chapter 22, Hacker Tools and Techniques by Ed Skoudis.
ISC2 OIG, 2007 p. 137-138, 419

QUESTION 247
Which of the following is unlike the other three choices presented?

A. El Gamal
B. Teardrop
C. Buffer Overflow
D. Smurf

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, pages 76, 157.

QUESTION 248
The standard server port number for HTTP is which of the following?

A. 81
B. 80
C. 8080
D. 8180

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: HTTP is Port 80.
MAIWALD, Eric, Network Security: A Beginner's Guide, McGraw-Hill/Osborne Media, 2001, page 135.

QUESTION 249
Which of the following are suitable protocols for securing VPN connections at the lower layers of the OSI model?

A. S/MIME and SSH
B. TLS and SSL
C. IPsec and L2TP
D. PKCS#10 and X.509

Correct Answer: C
Explanation

Explanation/Reference:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw- Hill/Osborne, page 467; SMITH, Richard E., Internet Cryptography, 1997, Addison-Wesley Pub Co.

QUESTION 250
What is the role of IKE within the IPsec protocol?

A. peer authentication and key exchange
B. data encryption
C. data signature
D. enforcing quality of service

Correct Answer: A
Explanation

Explanation/Reference:
RFC 2409: The Internet Key Exchange (IKE); DORASWAMY, Naganand & HARKINS, Dan, Ipsec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks, 1999, Prentice Hall PTR; SMITH, Richard E., Internet Cryptography, 1997, Addison-Wesley Pub Co.

QUESTION 251
What is NOT an authentication method within IKE and IPsec?

A. CHAP
B. Pre shared key
C. certificate based authentication
D. Public key authentication

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: CHAP is not used within IPSEC or IKE. CHAP is an authentication scheme used by Point to Point Protocol (PPP) servers to validate the identity of remote clients. CHAP periodically verifies the identity of the client by using a three-way handshake. This happens at the time of establishing the initial link (LCP), and may happen again at any time afterwards. The verification is based on a shared secret (such as the client user's password). After the completion of the link establishment phase, the authenticator sends a "challenge" message to the peer.
The peer responds with a value calculated using a one-way hash function on the challenge and the secret combined.
The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authenticator acknowledges the authentication; otherwise it should terminate the connection.
At random intervals the authenticator sends a new challenge to the peer and repeats steps 1 through 3.
The following were incorrect answers:
Pre Shared Keys
In cryptography, a pre-shared key or PSK is a shared secret which was previously shared between the two parties using some secure channel before it needs to be used. To build a key from shared secret, the key derivation function should be used. Such systems almost always use symmetric key cryptographic algorithms. The term PSK is used in WiFi encryption such as WEP or WPA, where both the wireless access points (AP) and all clients share the same key. The characteristics of this secret or key are determined by the system which uses it; some system designs require that such keys be in a particular format. It can be a password like 'bret13i', a passphrase like 'Idaho hung gear id gene', or a hexadecimal string like '65E4 E556 8622 EEE1'. The secret is used by all systems involved in the cryptographic processes used to secure the traffic between the systems.
Certificat Based Authentication
The most common form of trusted authentication between parties in the wide world of Web commerce is the exchange of certificates. A certificate is a digital document that at a minimum includes a Distinguished Name

(DN) and an associated public key. The certificate is digitally signed by a trusted third party known as the Certificate Authority (CA). The CA vouches for the authenticity of the certificate holder. Each principal in the transaction presents certificate as its credentials. The recipient then validates the certificate's signature against its cache of known and trusted CA certificates. A "personal certificate" identifies an end user in a transaction; a "server certificate" identifies the service provider.
Generally, certificate formats follow the X.509 Version 3 standard. X.509 is part of the Open Systems Interconnect
(OSI) X.500 specification.
Public Key Authentication
Public key authentication is an alternative means of identifying yourself to a login server, instead of typing a password. It is more secure and more flexible, but more difficult to set up. In conventional password authentication, you prove you are who you claim to be by proving that you know the correct password. The only way to prove you know the password is to tell the server what you think the password is. This means that if the server has been hacked, or spoofed an attacker can learn your password.
Public key authentication solves this problem. You generate a key pair, consisting of a public key (which everybody is allowed to know) and a private key (which you keep secret and do not give to anybody). The private key is able to generate signatures. A signature created using your private key cannot be forged by anybody who does not have a copy of that private key; but anybody who has your public key can verify that a particular signature is genuine. So you generate a key pair on your own computer, and you copy the public key to the server. Then, when the server asks you to prove who you are, you can generate a signature using your private key. The server can verify that signature (since it has your public key) and allow you to log in. Now if the server is hacked or spoofed, the attacker does not gain your private key or password; they only gain one signature. And signatures cannot be re-used, so they have gained nothing.
There is a problem with this: if your private key is stored unprotected on your own computer, then anybody who gains access to your computer will be able to generate signatures as if they were you. So they will be able to log in to your server under your account. For this reason, your private key is usually encrypted when it is stored on your local machine, using a passphrase of your choice. In order to generate a signature, you must decrypt the key, so you have to type your passphrase.

RFC 2409: The Internet Key Exchange (IKE); DORASWAMY, Naganand & HARKINS, Dan Ipsec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks, 1999, Prentice Hall PTR; SMITH, Richard E.
Internet Cryptography, 1997, Addison-Wesley Pub Co.; HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw-Hill/Osborne, page 467.
http://en.wikipedia.org/wiki/Pre-shared_key
http://www.home.umk.pl/~mgw/LDAP/RS.C4.JUN.97.pdf
http://the.earth.li/~sgtatham/putty/0.55/htmldoc/Chapter8.html#S8.1

QUESTION 252
In SSL/TLS protocol, what kind of authentication is supported when you establish a secure session between a client and a server?

A. Peer-to-peer authentication
B. Only server authentication (optional)
C. Server authentication (mandatory) and client authentication (optional)
D. Role based authentication scheme

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: RESCORLA, Eric, SSL and TLS: Designing and Building Secure Systems, 2000, Addison Wesley Professional; SMITH, Richard E., Internet Cryptography, 1997, Addison-Wesley Pub Co.

QUESTION 253
Which of the following is true of network security?

A. A firewall is a not a necessity in today's connected world.

B. A firewall is a necessity in today's connected world.
C. A whitewall is a necessity in today's connected world.
D. A black firewall is a necessity in today's connected world.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Commercial firewalls are a dime-a-dozen in todays world. Black firewall and whitewall are just distracters.

QUESTION 254
What is called the access protection system that limits connections by calling back the number of a previously authorized location?

A. Sendback systems
B. Callback forward systems
C. Callback systems
D. Sendback forward systems

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The
Answer: Call back Systems; Callback systems provide access protection by calling back the number of a previously authorized location, but this control can be compromised by call forwarding.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 35.

QUESTION 255
What is a decrease in amplitude as a signal propagates along a transmission medium best known as?

A. Crosstalk
B. Noise
C. Delay distortion
D. Attenuation

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Attenuation is the loss of signal strength as it travels. The longer a cable, the more at tenuation occurs, which causes the signal carrying the data to deteriorate. This is why standards include suggested cable-run lengths. If a networking cable is too long, attenuation may occur. Basically, the data are in the form of electrons, and these electrons have to "swim" through a copper wire. However, this is more like swimming upstream, because there is a lot of resistance on the electrons working in this media. After a certain distance, the electrons start to slow down and their encoding format loses form. If the form gets too degraded, the receiving system cannot interpret them any longer. If a network administrator needs to run a cable longer than its recommended segment length, she needs to insert a repeater or some type of device that will amplify the signal and ensure it gets to its destination in the right encoding format. Attenuation can also be caused by cable breaks and malfunctions. This is why cables should be tested. If a cable is suspected of attenuation problems, cable testers can inject signals into the cable and read the results at the end of the cable.
The following answers are incorrect:
Crosstalk - Crosstalk is one example of noise where unwanted electrical coupling between adjacent lines causes the signal in one wire to be picked up by the signal in an adjacent wire. Noise - Noise is also a signal

degradation but it refers to a large amount of electrical fluctuation that can interfere with the interpretation of the signal by the receiver. Delay distortion - Delay distortion can result in a misinterpretation of a signal that results from transmitting a digital signal with varying frequency components. The various components arrive at the receiver with varying delays.
Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 265
Official ISC2 guide to CISSP CBK 3rd Edition Page number 229 & CISSP All-In-One Exam guide 6th Edition Page Number 561

QUESTION 256
Which device acting as a translator is used to connect two networks or applications from layer 4 up to layer 7 of the ISO/OSI Model?

A. Bridge
B. Repeater
C. Router
D. Gateway

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: A gateway is used to connect two networks using dissimilar protocols at the lower layers or it could also be at the highest level of the protocol stack.
Important Note:
For the purpose of the exam, you have to remember that a gateway is not synonymous to the term firewall.
The second thing you must remembers is the fact that a gateway act as a translation device. It could be used to translate from IPX to TCP/IP for example. It could be used to convert different types of applications protocols and allow them to communicate together. A gateway could be at any of the OSI layers but usually tend to be higher up in the stack.
For your exam you should know the information below:
Repeaters
A repeater provides the simplest type of connectivity, because it only repeats electrical signals between cable segments, which enables it to extend a network. Repeaters work at the physical layer and are add-on devices for extending a network connection over a greater distance. The device amplifies signals because signals attenuate the farther they have to travel. Repeaters can also work as line conditioners by actually cleaning up the signals. This works much better when amplifying digital signals than when amplifying analog signals, because digital signals are discrete units, which makes extraction of background noise from them much easier for the amplifier. If the device is amplifying analog signals, any accompanying noise often is amplified as well, which may further distort the signal.
A hub is a multi-port repeater. A hub is often referred to as a concentrator because it is the physical communication device that allows several computers and devices to communicate with each other. A hub does not understand or work with IP or MAC addresses. When one system sends a signal to go to another system connected to it, the signal is broadcast to all the ports, and thus to all the systems connected to the concentrator.
Repeater

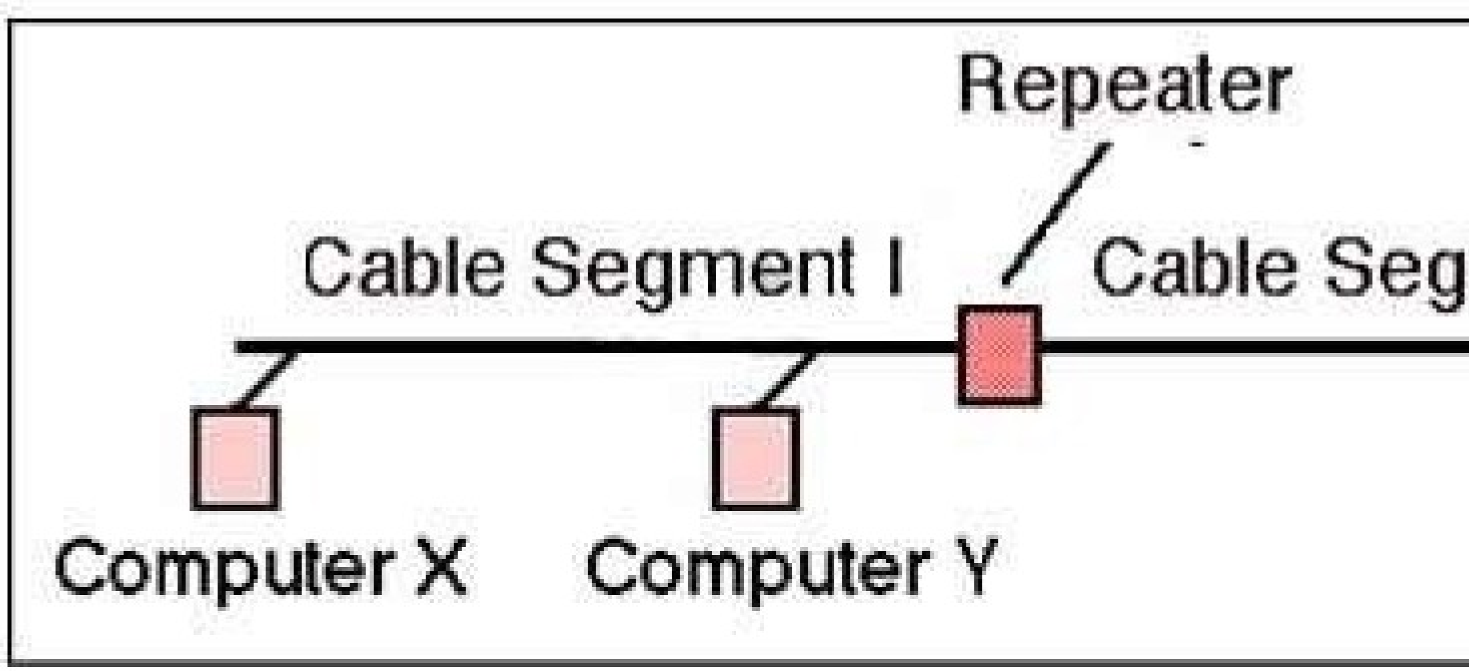


Image Reference- http://www.erg.abdn.ac.uk/~gorry/course/images/repeater.gif Bridges

A bridge is a LAN device used to connect LAN segments. It works at the data link layer and therefore works with MAC addresses. A repeater does not work with addresses; it just forwards all signals it receives. When a frame arrives at a bridge, the bridge determines whether or not the MAC address is on the local network segment. If the MAC address is not on the local network segment, the bridge forwards the frame to the necessary network segment.

Bridge

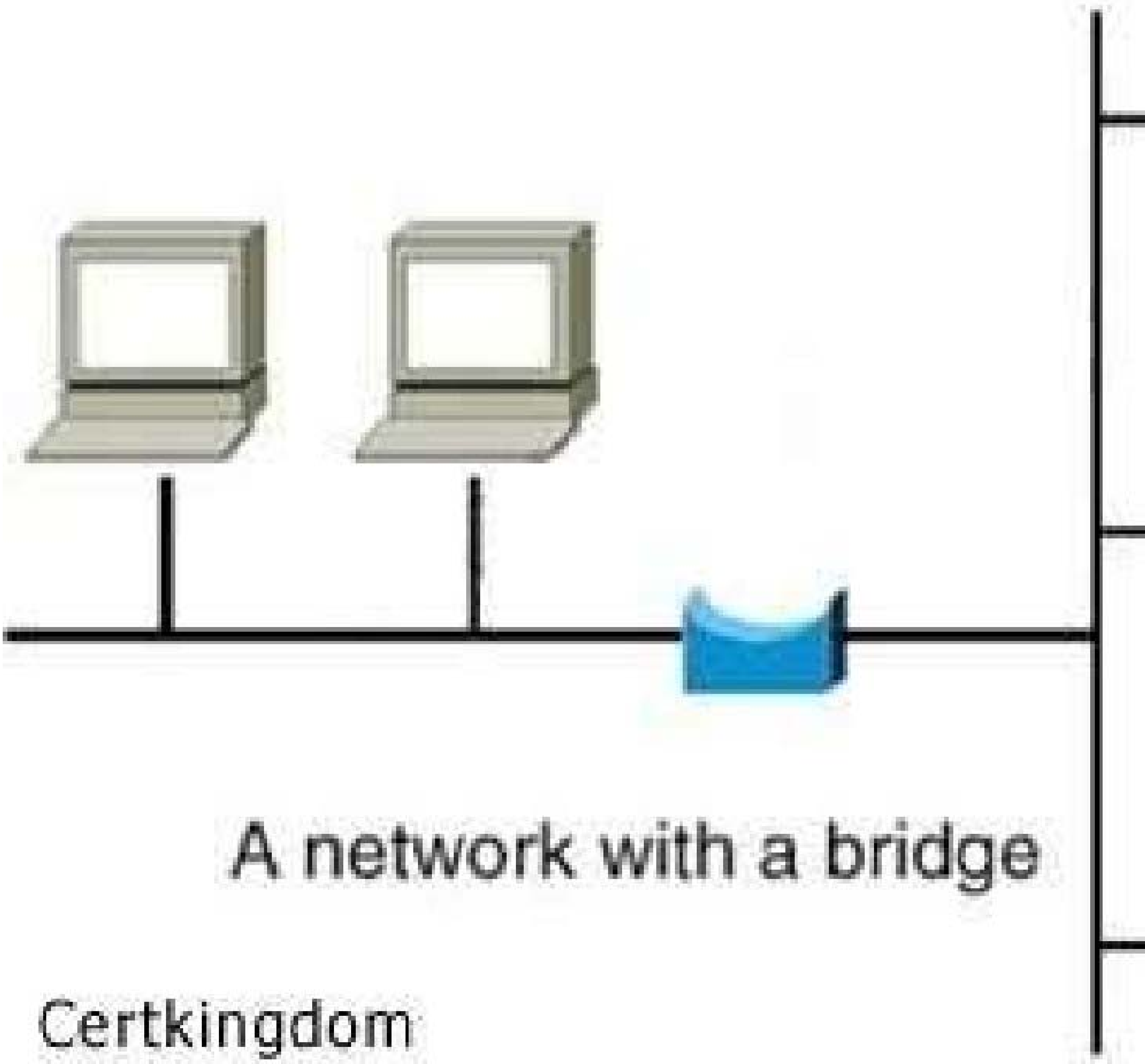


Image Reference- http://www.oreillynet.com/network/2001/01/30/graphics/bridge.jpg Routers
Routers are layer 3, or network layer, devices that are used to connect similar or different networks. (For example, they can connect two Ethernet LANs or an Ethernet LAN to a Token Ring LAN.) A router is a device that has two or more interfaces and a routing table so it knows how to get packets to their destinations. It can filter traffic based on access control lists (ACLs), and it fragments packets when necessary. Because routers have more network-level knowledge, they can perform higher-level functions, such as calculating the shortest and most economical path between the sending and receiving hosts.
Router and Switch

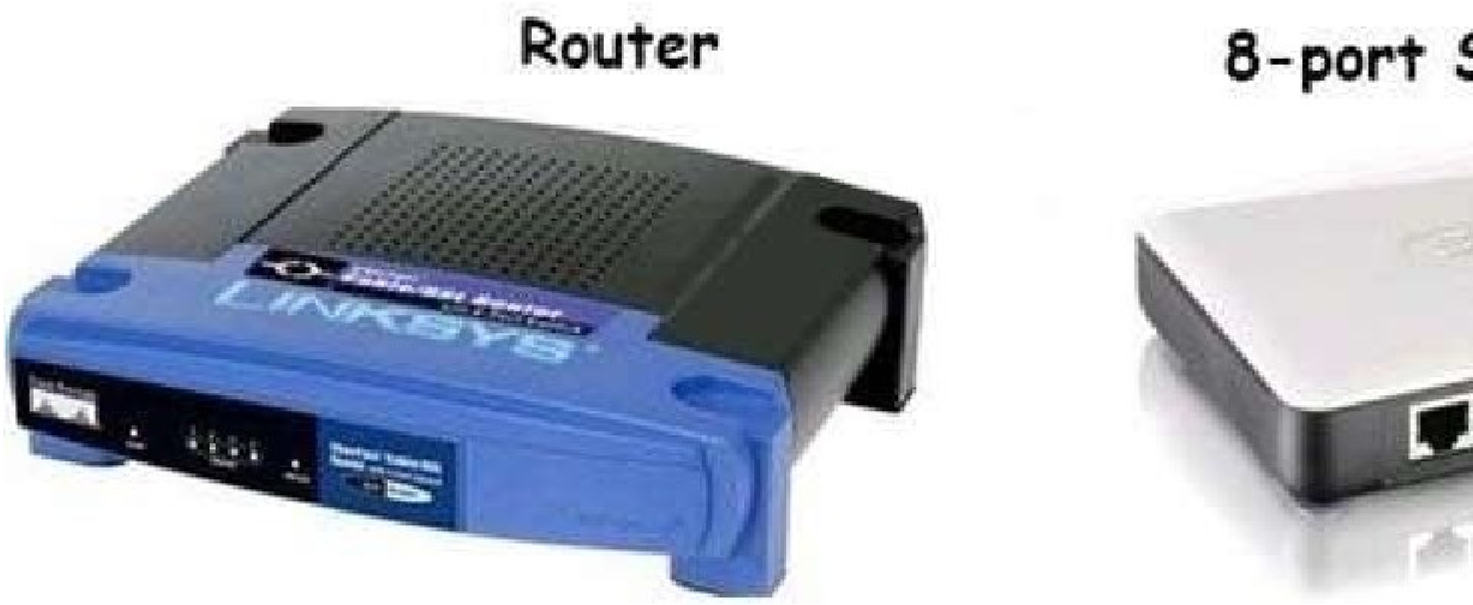


Image Reference- http://www.computer-networking-success.com/images/router-switch.jpg Switches

Switches combine the functionality of a repeater and the functionality of a bridge. A switch amplifies the electrical signal, like a repeater, and has the built-in circuitry and intelligence of a bridge. It is a multi-port connection device that provides connections for individual computers or other hubs and switches.

Gateways

Gateway is a general term for software running on a device that connects two different environments and that many times acts as a translator for them or somehow restricts their interactions. Usually a gateway is needed when one environment speaks a different language, meaning it uses a certain protocol that the other environment does not understand. The gateway can translate Internetwork Packet Exchange (IPX) protocol packets to IP packets, accept mail from one type of mail server and format it so another type of mail server can accept and understand it, or connect and translate different data link technologies such as FDDI to Ethernet.

Gateway Server

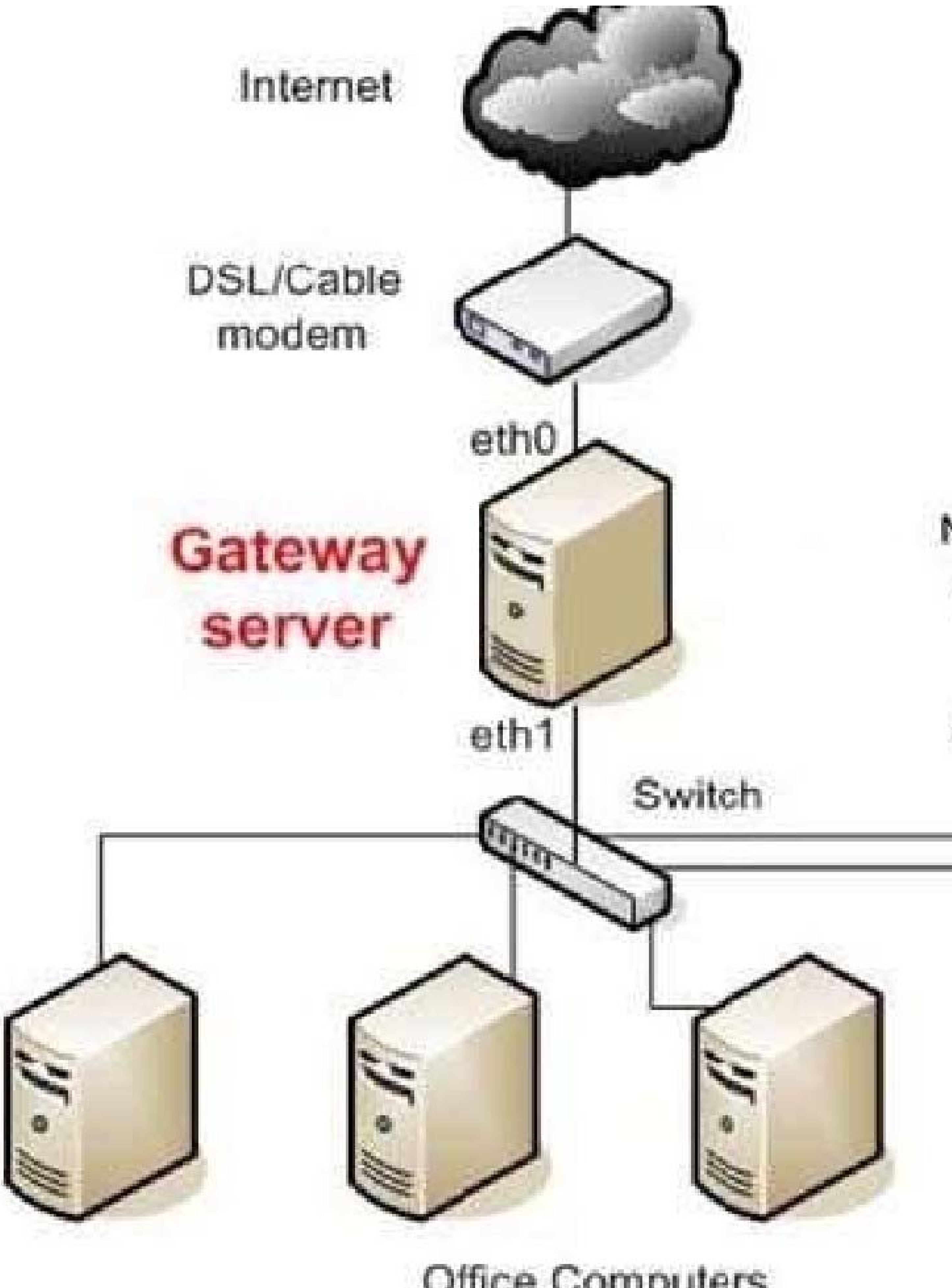

Internet
DSL/Cable modem
eth0
Gateway server
eth1
Switch
Office Computers

Image Referencehttp://
static.howtoforge.com/images/screenshots/556af08d5e43aa768260f9e589dc547f-3024.jpg The following answers are incorrect:
Repeater - A repeater provides the simplest type of connectivity, because it only repeats electrical signals between cable segments, which enables it to extend a network. Repeaters work at the physical layer and are add-on devices for extending a network connection over a greater distance. The device amplifies signals because signals attenuate the farther they have to travel. Bridges - A bridge is a LAN device used to connect LAN segments. It works at the data link layer and therefore works with MAC addresses. A repeater does not work with addresses; it just forwards all signals it receives. When a frame arrives at a bridge, the bridge determines whether or not the MAC address is on the local network segment. If the MAC address is not on the local network segment, the bridge forwards the frame to the necessary network segment. Routers - Routers are layer 3, or network layer, devices that are used to connect similar or different networks. (For example, they can connect two Ethernet LANs or an Ethernet LAN to a Token Ring LAN.) A router is a device that has two or more interfaces and a routing table so it knows how to get packets to their destinations. It can filter traffic based on access control lists (ACLs), and it fragments packets when necessary.
Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 263
Official ISC2 guide to CISSP CBK 3rd Edition Page number 229 and 230

QUESTION 257
In which layer of the OSI Model are connection-oriented protocols located in the TCP/IP suite of protocols?

A. Transport layer
B. Application layer
C. Physical layer
D. Network layer

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Connection-oriented protocols such as TCP provides reliability. It is the responsibility of such protocols in the transport layer to ensure every byte is accounted for. The network layer does not provide reliability. It only privides the best route to get the traffic to the final destination address.
For your exam you should know the information below about OSI model:
The Open Systems Interconnection model (OSI) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO), maintained by the identification ISO/IEC 7498-1. The model groups communication functions into seven logical layers. A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of that path. Two instances at one layer are connected by a horizontal.
OSI Model

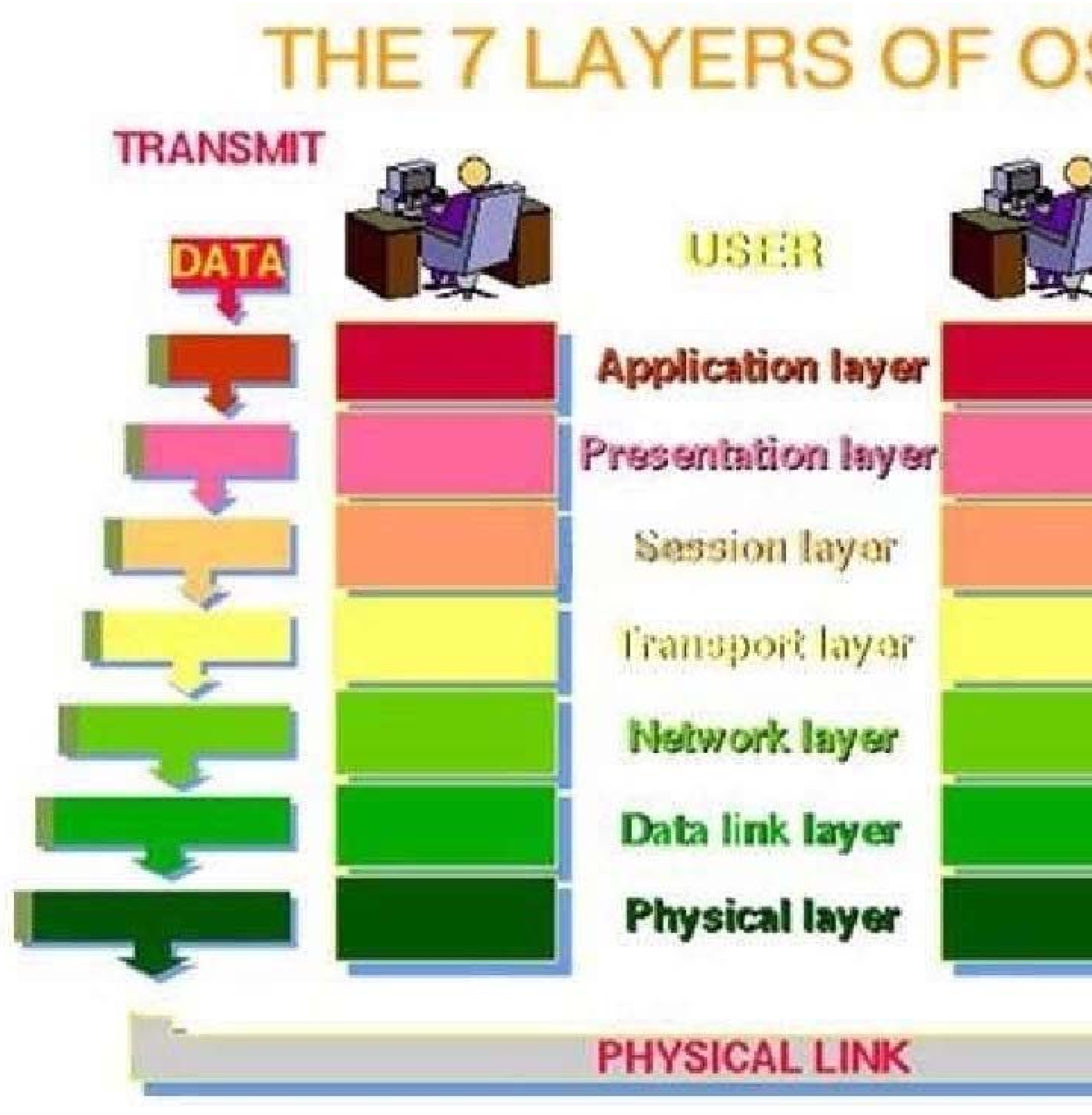


Image source: http://www.petri.co.il/images/osi_model.JPG PHYSICAL LAYER
The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides:
Data encoding: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. It determines:
What signal state represents a binary 1
How the receiving station knows when a "bit-time" starts How the receiving station delimits a frame
DATA LINK LAYER

The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link. To do this, the data link layer provides:

Link establishment and termination: establishes and terminates the logical link between two nodes.

Frame traffic control: tells the transmitting node to "back-off" when no frame buffers are available. Frame sequencing: transmits/receives frames sequentially. Frame acknowledgment: provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting non-acknowledged frames and handling duplicate frame receipt.

Frame delimiting: creates and recognizes frame boundaries. Frame error checking: checks received frames for integrity. Media access management: determines when the node "has the right" to use the physical medium.

NETWORK LAYER

The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors. It provides:

Routing: routes frames among networks.

Subnet traffic control: routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up. Frame fragmentation: if it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and reassembly at the destination station.

Logical-physical address mapping: translates logical addresses, or names, into physical addresses.

Subnet usage accounting: has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information.

Communications Subnet

The network layer software must build headers so that the network layer software residing in the subnet intermediate systems can recognize them and use them to route data to the destination address.

This layer relieves the upper layers of the need to know anything about the data transmission and intermediate switching technologies used to connect systems. It establishes, maintains and terminates connections across the intervening communications facility (one or several intermediate systems in the communication subnet).

In the network layer and the layers below, peer protocols exist between a node and its immediate neighbor, but the neighbor may be a node through which data is routed, not the destination station. The source and destination stations may be separated by many intermediate systems.

TRANSPORT LAYER

The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

The size and complexity of a transport protocol depends on the type of service it can get from the network layer. For a reliable network layer with virtual circuit capability, a minimal transport layer is required. If the network layer is unreliable and/or only supports datagrams, the transport protocol should include extensive error detection and recovery.

The transport layer provides:

Message segmentation: accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message. Message acknowledgment: provides reliable end-to-end message delivery with acknowledgments. Message traffic control: tells the transmitting station to "back-off" when no message buffers are available.

Session multiplexing: multiplexes several message streams, or sessions onto one logical link and keeps track of which messages belong to which sessions (see session layer). Typically, the transport layer can accept relatively large messages, but there are strict message size limits imposed by the network (or lower) layer. Consequently, the transport layer must break up the messages into smaller units, or frames, prepending a header to each frame. The transport layer header information must then include control information, such as message start and message end flags, to enable the transport layer on the other end to recognize message boundaries. In addition, if the lower layers do not maintain sequence, the transport header must contain sequence information to enable the transport layer on the receiving end to get the pieces back together in the right order before handing the received message up to the layer above.

End-to-end layers

Unlike the lower "subnet" layers whose protocol is between immediately adjacent nodes, the transport layer and the layers above are true "source to destination" or end-to-end layers, and are not concerned with the details of the underlying communications facility. Transport layer software (and software above it) on the source station carries on a conversation with similar software on the destination station by using message headers and control messages.

SESSION LAYER
The session layer allows session establishment between processes running on different stations.
It provides:
Session establishment, maintenance and termination: allows two application processes on different machines to establish, use and terminate a connection, called a session. Session support: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.
PRESENTATION LAYER
The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.
The presentation layer provides:
Character code translation: for example, ASCII to EBCDIC. Data conversion: bit order, CR-CR/LF, integer-floating point, and so on. Data compression: reduces the number of bits that need to be transmitted on the network. Data encryption: encrypt data for security purposes. For example, password encryption.
APPLICATION LAYER
The application layer serves as the window for users and application processes to access network services.
This layer contains a variety of commonly needed functions:
Resource sharing and device redirection
Remote file access
Remote printer access
Inter-process communication
Network management
Directory services
Electronic messaging (such as mail)
Network virtual terminals
The following were incorrect answers:
Application Layer - The application layer serves as the window for users and application processes to access network services.
Network layer - The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors. Physical Layer - The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers.
The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 260
and
Official ISC2 guide to CISSP CBK 3rd Edition Page number 287 and
http://en.wikipedia.org/wiki/Tcp_protocol

QUESTION 258
Which of the following is a telecommunication device that translates data from digital to analog form and back to digital?

A. Multiplexer
B. Modem
C. Protocol converter
D. Concentrator

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: A modem is a device that translates data from digital form and then back to digital for communication over analog lines.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 3: Technical Infrastructure and Operational Practices (page 114).

QUESTION 259

Which of the following transmission media would NOT be affected by cross talk or interference?

A. Copper cable
B. Radio System
C. Satellite radiolink
D. Fiber optic cables

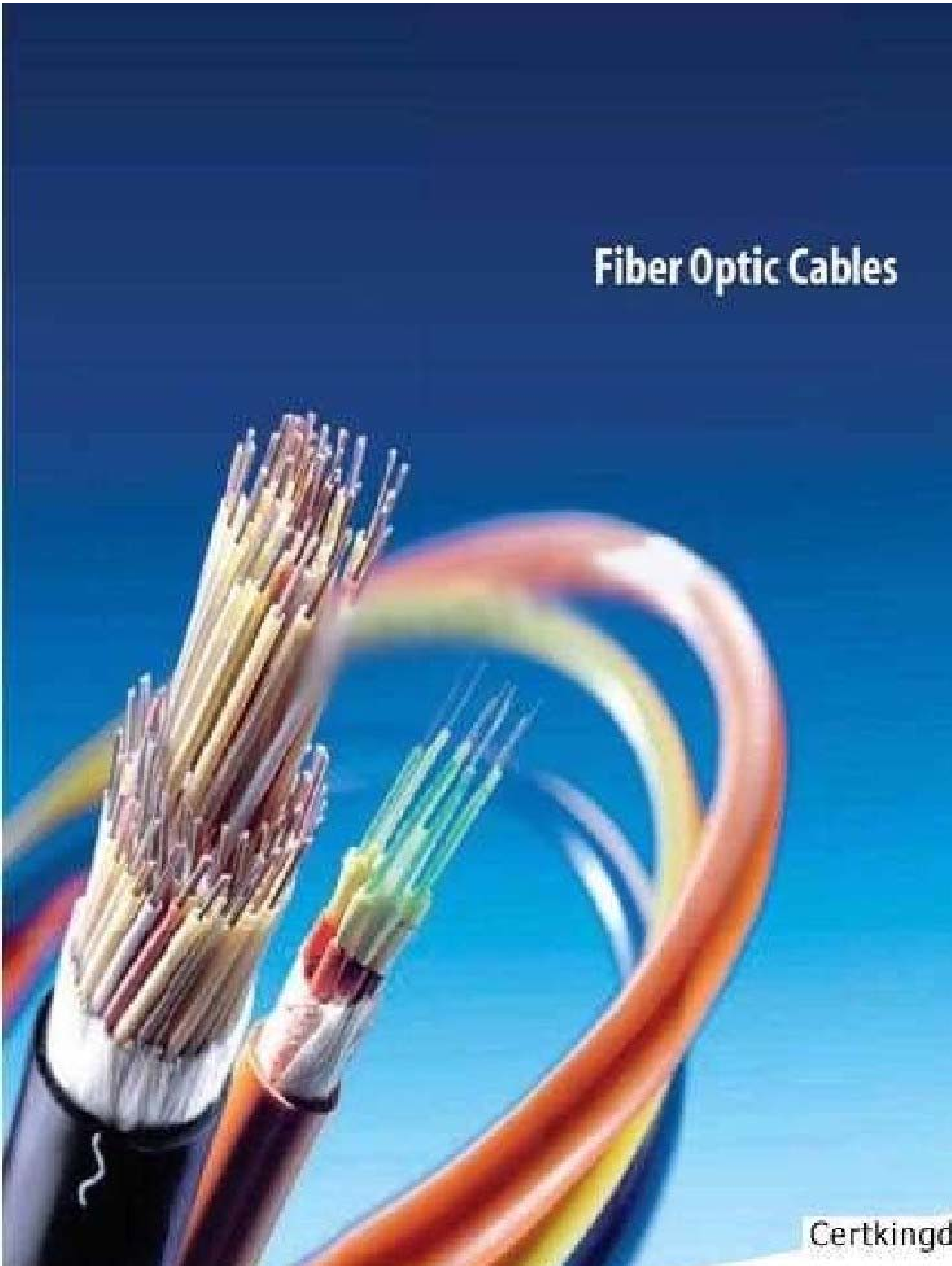
Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Only fiber optic cables are not affected by crosstalk or interference. For your exam you should know the information about transmission media:
Copper Cable
Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.
Copper has been used in electric wiring since the invention of the electromagnet and the telegraph in the 1820s.The invention of the telephone in 1876 created further demand for copper wire as an electrical conductor.
Copper is the electrical conductor in many categories of electrical wiring. Copper wire is used in power generation, power transmission, power distribution, telecommunications, electronics circuitry, and countless types of electrical equipment. Copper and its alloys are also used to make electrical contacts. Electrical wiring in buildings is the most important market for the copper industry. Roughly half of all copper mined is used to manufacture electrical wire and cable conductors.
Copper Cable

Certki

Image Source - http://i00.i.aliimg.com/photo/v0/570456138/FRLS_HR_PVC_Copper_Cable.jpg Coaxial cable
Coaxial cable, or coax (pronounced 'ko.aks), is a type of cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield. Many coaxial cables also have an insulating outer sheath or jacket. The term coaxial comes from the inner conductor and the outer shield sharing a geometric axis. Coaxial cable was invented by English engineer and mathematician Oliver Heaviside, who patented the design in 1880.Coaxial cable differs from other shielded cable used for carrying lower-frequency signals, such as audio signals, in that the dimensions of the cable are controlled to give a precise, constant conductor spacing, which is needed for it to function efficiently as a radio frequency transmission line. Coaxial cable are expensive and does not support many LAN's. It supports data and video
Coaxial Cable

Image Source - http://www.tlc-direct.co.uk/Images/Products/size_3/CARG59.JPG Fiber optics
An optical fiber cable is a cable containing one or more optical fibers that are used to carry light. The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed. Different types of cable are used for different applications, for example long distance telecommunication, or providing a high-speed data connection between different parts of a building. Fiber optics used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.
Radio System
Radio systems are used for short distance,cheap and easy to tap. Radio is the radiation (wireless transmission) of electromagnetic signals through the atmosphere or free space.
Information, such as sound, is carried by systematically changing (modulating) some property of the radiated waves, such as their amplitude, frequency, phase, or pulse width. When radio waves strike an electrical conductor, the oscillating fields induce an alternating current in the conductor. The information in the waves can be extracted and transformed back into its original form.
Fiber Optics



Fiber Optic Cables

Image Source - http://aboveinfranet.com/wp-content/uploads/2014/04/fiber-optic-cables-aboveinfranet-solutions.jpg

Microwave radio system

Microwave transmission refers to the technology of transmitting information or energy by the use of radio waves whose wavelengths are conveniently measured in small numbers of centimetre; these are called microwaves.

Microwaves are widely used for point-to-point communications because their small wavelength allows conveniently-sized antennas to direct them in narrow beams, which can be pointed directly at the receiving antenna. This allows nearby microwave equipment to use the same frequencies without interfering with each other, as lower frequency radio waves do. Another advantage is that the high frequency of microwaves gives the microwave band a very large information-carrying capacity; the microwave band has a bandwidth 30 times that of all the rest of the radio spectrum below it. A disadvantage is that microwaves are limited to line of sight propagation; they cannot pass around hills or mountains as lower frequency radio waves can. Microwave radio transmission is commonly used in point-to-point communication systems on the surface of the Earth, in satellite communications, and in deep space radio communications. Other parts of the microwave radio band are used for radars, radio navigation systems, sensor systems, and radio astronomy.

Microwave radio systems are carriers for voice data signal, cheap and easy to tap.

Microwave Radio System

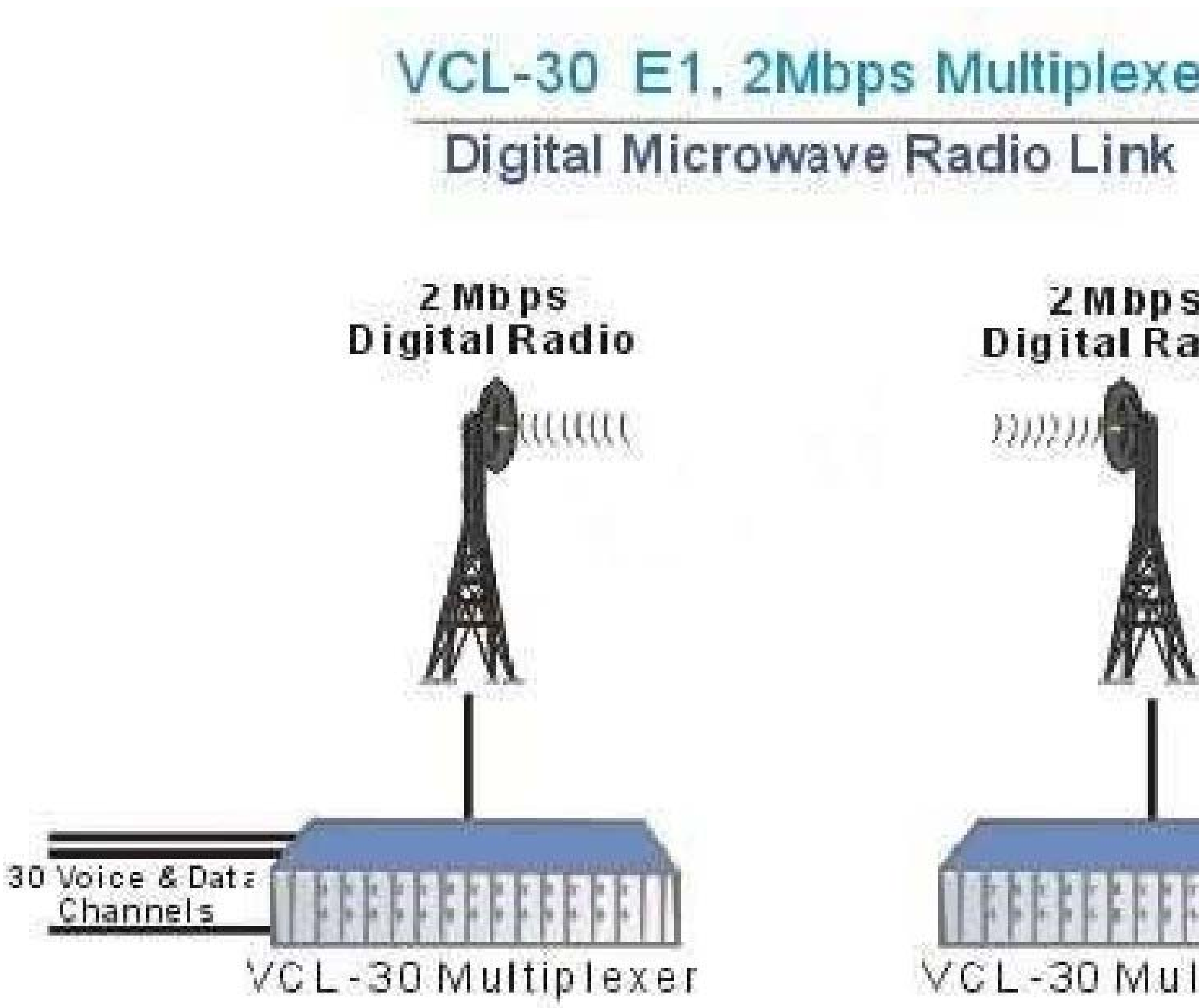


Image Source - http://www.valiantcom.com/images/applications/e1_digital_microwave_radio.gif Satellite Radio Link
Satellite radio is a radio service broadcast from satellites primarily to cars, with the signal broadcast nationwide, across a much wider geographical area than terrestrial radio stations. It is available by subscription, mostly commercial free, and offers subscribers more stations and a wider variety of programming options than terrestrial radio. Satellite radio link uses transponder to send information and easy to tap.
The following answers are incorrect:
Copper Cable - Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.
Radio System - Radio systems are used for short distance,cheap and easy to tap. Satellite Radio Link - Satellite radio link uses transponder to send information and easy to tap. The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 265 &
Official ISC2 guide to CISSP CBK 3rd Edition Page number 233

QUESTION 260
What is called an attack where the attacker spoofs the source IP address in an ICMP ECHO broadcast packet

so it seems to have originated at the victim's system, in order to flood it with REPLY packets?

A. SYN Flood attack
B. Smurf attack
C. Ping of Death attack
D. Denial of Service (DOS) attack

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Although it may cause a denial of service to the victim's system, this type of attack is a Smurf attack. A SYN Flood attack uses up all of a system's resources by setting up a number of bogus communication sockets on the victim's system. A Ping of Death attack is done by sending IP packets that exceed the maximum legal length (65535 octets). Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 11: Application and System Development (page 789).

QUESTION 261
What is the main difference between a Smurf and a Fraggle attack?

A. A Smurf attack is ICMP-based and a Fraggle attack is UDP-based.
B. A Smurf attack is UDP-based and a Fraggle attack is TCP-based.
C. Smurf attack packets cannot be spoofed.
D. A Smurf attack is UDP-based and a Fraggle attack is ICMP-based.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Fraggle is an attack similar to Smurf, but instead of using ICMP, it uses UDP. Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 11: Application and System Development (page 790).

QUESTION 262
Why are coaxial cables called "coaxial"?

A. it includes two physical channels that carries the signal surrounded (after a layer of insulation) by another concentric physical channel, both running along the same axis.
B. it includes one physical channel that carries the signal surrounded (after a layer of insulation) by another concentric physical channel, both running along the same axis
C. it includes two physical channels that carries the signal surrounded (after a layer of insulation) by another two concentric physical channels, both running along the same axis.
D. it includes one physical channel that carries the signal surrounded (after a layer of insulation) by another concentric physical channel, both running perpendicular and along the different axis

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Coaxial cable is called "coaxial" because it includes one physical channel that carries the signal surrounded (after a layer of insulation) by another concentric physical channel, both running along the same axis.
The outer channel serves as a ground. Many of these cables or pairs of coaxial tubes can be placed in a single outer sheathing and, with repeaters, can carry information for a great distance. Source: STEINER, Kurt, Telecommunications and Network Security, Version 1, May 2002, CISSP Open Study Group (Domain Leader: skottikus), Page 14.

QUESTION 263
The International Standards Organization / Open Systems Interconnection (ISO/OSI) Layers does NOT have which of the following characteristics?

A. Standard model for network communications
B. Used to gain information from network devices such as count of packets received and routing tables
C. Enables dissimilar networks to communicate
D. Defines 7 protocol layers (a.k.a. protocol stack)

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The International Standards Organization / Open Systems Interconnection (ISO/OSI) Layers and Characteristics Standard model for network communications enables dissimilar networks to communicate, Defines 7 protocol layers (a.k.a. protocol stack) Each layer on one workstation communicates with its respective layer on another workstation using protocols (i.e. agreed-upon communication formats) "Mapping" each protocol to the model is useful for comparing protocols.
Mnemonics: Please Do Not Throw Sausage Pizza Away (bottom to top layer) All People Seem To Need Data Processing (top to bottom layer). Source: STEINER, Kurt, Telecommunications and Network Security, Version 1, May 2002, CISSP Open Study Group (Domain Leader: skottikus), Page 12.

QUESTION 264
In telephony different types of connections are being used. The connection from the phone company's branch office to local customers is referred to as which of the following choices?

A. new loop
B. local loop
C. loopback
D. indigenous loop

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Transmission on fiber optic wire requires repeating at distance intervals. The glass fiber requires more protection within an outer cable than copper. For these reasons and because the installation of any new wiring is labor-intensive, few communities yet have fiber optic wires or cables from the phone company's branch office to local customers (local loop). In telephony, a local loop is the wired connection from a telephone company's central office in a locality to its customers' telephones at homes and businesses. This connection is usually on a pair of copper wires called twisted pair. The system was originally designed for voice transmission only using analog transmission technology on a single voice channel. Today, your computer's modem makes the conversion between analog signals and digital signals. With Integrated Services Digital Network (ISDN) or Digital Subscriber Line (DSL), the local loop can carry digital signals directly and at a much higher bandwidth than they do for voice only.
Local Loop diagram

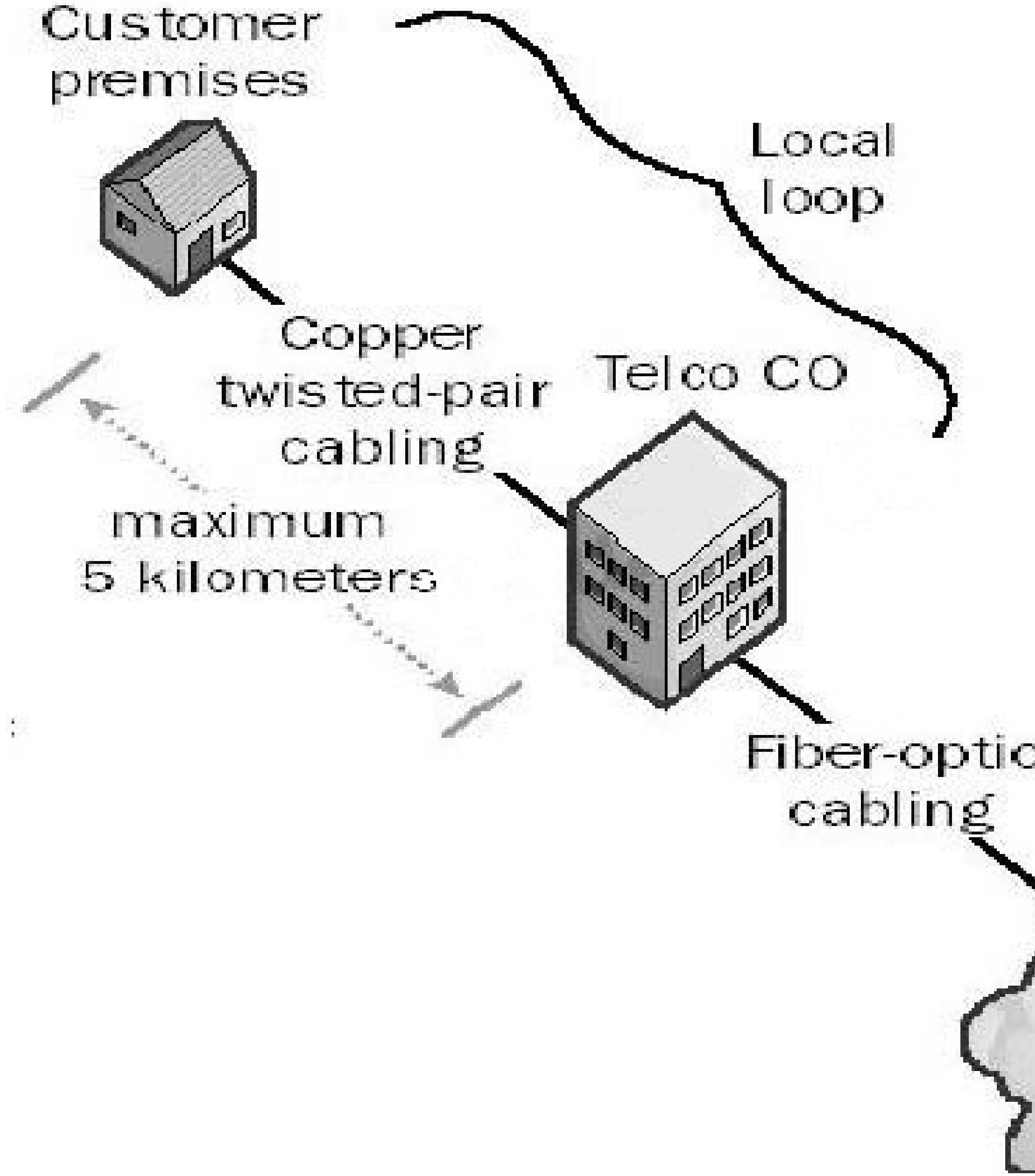


Image from: http://www.thenetworkencyclopedia.com/entry/local-loop/ The following are incorrect answers:

New loop This is only a detractor and does not exist
Loopback In telephone systems, a loopback is a test signal sent to a network destination that is returned as received to the originator. The returned signal may help diagnose a problem. Ingenious loop This is only a detractor and does not exist Reference(s) used for this question:
http://searchnetworking.techtarget.com/definition/local-loop and
STEINER, Kurt, Telecommunications and Network Security, Version 1, May 2002, CISSP Open Study Group (Domain Leader: skottikus), Page 14.

QUESTION 265
Communications and network security relates to transmission of which of the following?

A. voice
B. voice and multimedia
C. data and multimedia
D. voice, data and multimedia

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: From the published (ISC)2 goals for the Certified Information Systems Security Professional candidate:
The CISSP candidate should be familiar to communications and network security as it relates to voice, data, multimedia, and facsimile transmissions in terms of local area, wide area, and remote access.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 57.

QUESTION 266
One of the following statements about the differences between PPTP and L2TP is NOT true

A. PPTP can run only on top of IP networks.
B. PPTP is an encryption protocol and L2TP is not.
C. L2TP works well with all firewalls and network devices that perform NAT.
D. L2TP supports AAA servers

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: L2TP is affected by packet header modification and cannot cope with firewalls and network devices that perform NAT.
"PPTP can run only on top of IP networks." is correct as PPTP encapsulates datagrams into an IP packet, allowing PPTP to route many network protocols across an IP network. "PPTP is an encryption protocol and L2TP is not." is correct. When using PPTP, the PPP payload is encrypted with Microsoft Point-to-Point Encryption (MPPE) using MSCHAP or EAP-TLS. "L2TP supports AAA servers" is correct as L2TP supports TACACS+ and RADIUS.
NOTE:
L2TP does work over NAT. It is possible to use a tunneled mode that wraps every packet into a UDP packet. Port 4500 is used for this purpose. However this is not true of PPTP and it is not true as well that it works well with all firewalls and NAT devices.

All in One Third Edition page 545
Official Guide to the CISSP Exam page 124-126

QUESTION 267
You have been tasked to develop an effective information classification program. Which one of the following steps should be performed first?

A. Establish procedures for periodically reviewing the classification and ownership
B. Specify the security controls required for each classification level
C. Identify the data custodian who will be responsible for maintaining the security level of data
D. Specify the criteria that will determine how data is classified

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: According to the AIO 3rd edition, these are the necessary steps for a proper classification program:
1. Define classification levels.
2. Specify the criteria that will determine how data is classified.
3. Have the data owner indicate the classification of the data she is responsible for.
4. Identify the data custodian who will be responsible for maintaining data and its security level.
5. Indicate the security controls, or protection mechanisms, that are required for each classification level.
6. Document any exceptions to the previous classification issues.
7. Indicate the methods that can be used to transfer custody of the information to a different data owner.
8. Create a procedure to periodically review the classification and ownership. Communicate any changes to the data custodian.
9. Indicate termination procedures for declassifying the data.
10. Integrate these issues into the security-awareness program so that all employees understand how to handle data at different classification levels.
Domain: Information security and risk management
AIO 3rd edition page 50

QUESTION 268
A group of independent servers, which are managed as a single system, that provides higher availability, easier manageability, and greater scalability is:

A. server cluster
B. client cluster
C. guest cluster
D. host cluster

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: A server cluster is a group of independent servers, which are managed as a single system, that provides higher availability, easier manageability, and greater scalability. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 67.

QUESTION 269
A server cluster looks like a:

A. single server from the user's point of view
B. dual server from the user's point of view
C. triple server from the user's point of view
D. quardle server from the user's point of view

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The cluster looks like a single server from the user's point of view. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 67.

QUESTION 270
If any server in the cluster crashes, processing continues transparently, however, the cluster suffers some performance degradation. This implementation is sometimes called a:

A. server farm
B. client farm
C. cluster farm
D. host farm

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: If any server in the cluster crashes, processing continues transparently, however, the cluster suffers some performance degradation. This implementation is sometimes called a "server farm."
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 67.

QUESTION 271
Which of the following is immune to the effects of electromagnetic interference (EMI) and therefore has a much longer effective usable length?

A. Fiber Optic cable
B. Coaxial cable
C. Twisted Pair cable
D. Axial cable

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Fiber Optic cable is immune to the effects of electromagnetic interference (EMI) and therefore has a much longer effective usable length (up to two kilometers in some cases). Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 72.

QUESTION 272
Which of the following methods of providing telecommunications continuity involves the use of an alternative media?

A. Alternative routing
B. Diverse routing
C. Long haul network diversity
D. Last mile circuit protection

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Alternative routing is a method of routing information via an alternate medium such as copper cable or fiber optics. This involves use of different networks, circuits or end points should the normal network

be unavailable. Diverse routing routes traffic through split cable facilities or duplicate cable facilities. This can be accomplished with different and/or duplicate cable sheaths. If different cable sheaths are used, the cable may be in the same conduit and therefore subject to the same interruptions as the cable it is backing up. The communication service subscriber can duplicate the facilities by having alternate routes, although the entrance to and from the customer premises may be in the same conduit. The subscriber can obtain diverse routing and alternate routing from the local carrier, including dual entrance facilities. This type of access is time-consuming and costly. Long haul network diversity is a diverse long-distance network utilizing T1 circuits among the major long-distance carriers. It ensures long-distance access should any one carrier experience a network failure. Last mile circuit protection is a redundant combination of local carrier T1s microwave and/or coaxial cable access to the local communications loop. This enables the facility to have access during a local carrier communication disaster. Alternate local carrier routing is also utilized. Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 5: Disaster Recovery and Business Continuity (page 259).

QUESTION 273
Which port does the Post Office Protocol Version 3 (POP3) make use of?

A. 110
B. 109
C. 139
D. 119

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The other answers are not correct because of the following protocol/port numbers matrix:
Post Office Protocol (POP2) 109
Network News Transfer Protocol 119
NetBIOS 139

QUESTION 274
Which of the following are WELL KNOWN PORTS assigned by the IANA?

A. Ports 0 to 255
B. Ports 0 to 1024
C. Ports 0 to 1023
D. Ports 0 to 127

Correct Answer: C
Explanation

Explanation/Reference:
The port numbers are divided into three ranges: the Well Known Ports, the Registered Ports, and the Dynamic and/or Private Ports. The range for assigned "Well Known" ports managed by the IANA (Internet Assigned Numbers Authority) is 0-1023.
Source: iana.org: port assignments.

QUESTION 275
Which of the following are REGISTERED PORTS as defined by IANA ?

A. Ports 128 to 255
B. Ports 1024 to 49151
C. Ports 1025 to 65535
D. Ports 1024 to 32767

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Ports 1024 to 49151 has been defined as REGISTERED PORTS by IANA. A registered port is a network port (a sub-address defined within the Internet Protocol, in the range 165535) assigned by the Internet Assigned Numbers Authority (IANA) (or by Internet Corporation for Assigned Names and Numbers (ICANN) before March 21, 2001) for use with a certain protocol or application.
Ports with numbers lower than those of the registered ports are called well known ports; ports with numbers greater than those of the registered ports are called dynamic and/or private ports.
Ports 0-1023 - well known ports
Ports 1024-49151 - Registered port: vendors use for applications Ports >49151 - dynamic / private ports
The other answers are not correct
Reference(s) used for this question:
http://en.wikipedia.org/wiki/Registered_port

QUESTION 276
Which of the following countermeasures would be the most appropriate to prevent possible intrusion or damage from wardialing attacks?

A. Monitoring and auditing for such activity
B. Require user authentication
C. Making sure only necessary phone numbers are made public
D. Using completely different numbers for voice and data accesses

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Knowlege of modem numbers is a poor access control method as an attacker can discover modem numbers by dialing all numbers in a range. Requiring user authentication before remote access is granted will help in avoiding unauthorized access over a modem line. "Monitoring and auditing for such activity" is incorrect. While monitoring and auditing can assist in detecting a wardialing attack, they do not defend against a successful wardialing attack. "Making sure that only necessary phone numbers are made public" is incorrect. Since a wardialing attack blindly calls all numbers in a range, whether certain numbers in the range are public or not is irrelevant.
"Using completely different numbers for voice and data accesses" is incorrect. Using different number ranges for voice and data access might help prevent an attacker from stumbling across the data lines while wardialing the public voice number range but this is not an adequate countermeaure.

CBK, p. 214
AIO3, p. 534-535

QUESTION 277
What is the maximum length of cable that can be used for a twisted-pair, Category 5 10Base-T cable?

A. 80 meters
B. 100 meters
C. 185 meters
D. 500 meters

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: As a signal travels though a medium, it attenuates (loses strength) and at some point will become indistinguishable from noise. To assure trouble-free communication, maximum cable lengths are set between

nodes to assure that attenuation will not cause a problem. The maximum CAT-5 UTP cable length between two nodes for 10BASE-T is 100M.
The following answers are incorrect:
80 meters. It is only a distracter.
185 meters. Is incorrect because it is the maximum length for 10Base-2 500 meters. Is incorrect because it is the maximum length for 10Base-5

QUESTION 278
What type of cable is used with 100Base-TX Fast Ethernet?

A. Fiber-optic cable
B. Category 3 or 4 unshielded twisted-pair (UTP).
C. Category 5 unshielded twisted-pair (UTP).
D. RG-58 cable.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: This is the type of cabling recommended for 100Base-TX networks. Fiber-optic cable is incorrect. Incorrect media type for 100Base-TX -- 100Base-FX would denote fiber optic cabling.
"Category 3 or 4 unshielded twisted-pair (UTP)" is incorrect. These types are not recommended for 100Mbps operation.
RG-58 cable is incorrect. Incorrect media type for 100Base-TX.
References
CBK, p. 428
AIO3, p. 455

QUESTION 279
Secure Sockets Layer (SSL) is very heavily used for protecting which of the following?

A. Web transactions.
B. EDI transactions.
C. Telnet transactions.
D. Electronic Payment transactions.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: SSL was developed Netscape Communications Corporation to improve security and privacy of HTTP transactions.
SSL is one of the most common protocols used to protect Internet traffic. It encrypts the messages using symmetric algorithms, such as IDEA, DES, 3DES, and Fortezza, and also calculates the MAC for the message using MD5 or SHA-1. The MAC is appended to the message and encrypted along with the message data.
The exchange of the symmetric keys is accomplished through various versions of DiffieHellmann or RS
A. TLS is the Internet standard based on SSLv3. TLSv1 is backward compatible with SSLv3. It uses the same algorithms as SSLv3; however, it computes an HMAC instead of a MAC along with other enhancements to improve security.
The following are incorrect answers:
"EDI transactions" is incorrect. Electronic Data Interchange (EDI) is not the best answer to this question though SSL could play a part in some EDI transactions. "Telnet transactions" is incorrect. Telnet is a character mode protocol and is more likely to be secured by Secure Telnet or replaced by the Secure Shell (SSH) protocols.
"Eletronic payment transactions" is incorrect. Electronic payment is not the best answer to this question though SSL could play a part in some electronic payment transactions.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press)

(Kindle Locations 16615-16619). Auerbach Publications. Kindle Edition.
and
http://en.wikipedia.org/wiki/Transport_Layer_Security

QUESTION 280
Secure Shell (SSH) is a strong method of performing:

A. client authentication
B. server authentication
C. host authentication
D. guest authentication

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Secure shell (SSH) was designed as an alternative to some of the insecure protocols and allows users to securely access resources on remote computers over an encrypted tunnel. The Secure Shell Protocol (SSH) is a protocol for secure remote login and other secure network services over an insecure network. The SSH authentication protocol runs on top of the SSH transport layer protocol and provides a single authenticated tunnel for the SSH connection protocol.
SSH's services include remote log-on, file transfer, and command execution. It also supports port forwarding, which redirects other protocols through an encrypted SSH tunnel. Many users protect less secure traffic of protocols, such as X Windows and VNC (virtual network computing), by forwarding them through a SSH tunnel.
The SSH tunnel protects the integrity of communication, preventing session hijacking and other man-in-the-middle attacks. Another advantage of SSH over its predecessors is that it supports strong authentication. There are several alternatives for SSH clients to authenticate to a SSH server, including passwords and digital certificates.
Keep in mind that authenticating with a password is still a significant improvement over the other protocols because the password is transmitted encrypted. There are two incompatible versions of the protocol, SSH-1 and SSH-2, though many servers support both. SSH-2 has improved integrity checks (SSH-1 is vulnerable to an insertion attack due to weak CRC-32 integrity checking) and supports local extensions and additional types of digital certificates such as Open PGP. SSH was originally designed for UNIX, but there are now implementations for other operating systems, including Windows, Macintosh, and OpenVMS.
Is SSH 3.0 the same as SSH3?
The short answer is: NO SSH 3.0 refers to version 3 of SSH Communications SSH2 protocol implementation and it could also refer to OpenSSH Version 3.0 of its SSH2 software. The "3" refers to the software release version not the protocol version. As of this writing (July 2013), there is no SSH3 protocol.
"Server authentication" is incorrect. Though many SSH clients allow pre-caching of server/host keys, this is a minimal form of server/host authentication. "Host authentication" is incorrect. Though many SSH clients allow pre-caching of server/host keys, this is a minimal form of server/host authentication.
"Guest authentication" is incorrect. The general idea of "guest" is that it is unauthenticated access.
Reference(s) used for this question:
http://www.ietf.org/rfc/rfc4252.txt
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 7080-7088). Auerbach Publications. Kindle Edition.

QUESTION 281
Secure Shell (SSH-2) supports authentication, compression, confidentiality, and integrity, SSH is commonly used as a secure alternative to all of the following protocols below except:

A. telnet
B. rlogin
C. RSH
D. HTTPS

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: HTTPS is used for secure web transactions and is not commonly replaced by SSH. Users often want to log on to a remote computer. Unfortunately, most early implementations to meet that need were designed for a trusted network. Protocols/programs, such as TELNET, RSH, and rlogin, transmit unencrypted over the network, which allows traffic to be easily intercepted. Secure shell (SSH) was designed as an alternative to the above insecure protocols and allows users to securely access resources on remote computers over an encrypted tunnel. SSH's services include remote log-on, file transfer, and command execution. It also supports port forwarding, which redirects other protocols through an encrypted SSH tunnel. Many users protect less secure traffic of protocols, such as X Windows and VNC (virtual network computing), by forwarding them through a SSH tunnel. The SSH tunnel protects the integrity of communication, preventing session hijacking and other man-in-the-middle attacks. Another advantage of SSH over its predecessors is that it supports strong authentication. There are several alternatives for SSH clients to authenticate to a SSH server, including passwords and digital certificates. Keep in mind that authenticating with a password is still a significant improvement over the other protocols because the password is transmitted encrypted.
The following were wrong answers:
telnet is an incorrect choice. SSH is commonly used as an more secure alternative to telnet. In fact Telnet should not longer be used today.
rlogin is and incorrect choice. SSH is commonly used as a more secure alternative to rlogin. RSH is an incorrect choice. SSH is commonly used as a more secure alternative to RSH.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 7077-7088). Auerbach Publications. Kindle Edition.

QUESTION 282
Secure Shell (SSH-2) provides all the following services except:

A. secure remote login
B. command execution
C. port forwarding
D. user authentication

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: This is one of the tricky negative question. You have to pay close attention to the word EXCEPT within the question.
The SSH transport layer is a secure, low level transport protocol. It provides strong encryption, cryptographic host authentication, and integrity protection. Authentication in this protocol level is host-based; this protocol does not perform user authentication. A higher level protocol for user authentication can be designed on top of this protocol.
The protocol has been designed to be simple and flexible to allow parameter negotiation, and to minimize the number of round-trips. The key exchange method, public key algorithm, symmetric encryption algorithm, message authentication algorithm, and hash algorithm are all negotiated. It is expected that in most environments, only 2 round-trips will be needed for full key exchange, server authentication, service request, and acceptance notification of service request. The worst case is 3 round-trips.
The following are incorrect answers:
"Remote log-on" is incorrect. SSH does provide remote log-on. "Command execution" is incorrect. SSH does provide command execution. "Port forwarding" is incorrect. SSH does provide port forwarding. SSH also has a wonderful feature called SSH Port Forwarding, sometimes called SSH Tunneling, which allows you to establish a secure SSH session and then tunnel arbitrary TCP connections through it. Tunnels can be created at any time, with almost no effort and no programming, which makes them very appealing. See the article below in the reference to take a look at SSH Port Forwarding in detail, as it is a very useful but often misunderstood technology. SSH Port Forwarding can be used for secure communications in a myriad of different ways.
You can see a nice tutorial on the PUTTY web site on how to use PUTTY to do port forwarding at:

http://www.cs.uu.nl/technical/services/ssh/putty/puttyfw.html Reference(s) used for this question:
RFC 4253 at https://www.ietf.org/rfc/rfc4253.txt
and
SSH Port Forwarding by Symantec

QUESTION 283
Transport Layer Security (TLS) is a two-layered socket layer security protocol that contains the TLS Record Protocol and the::

A. Transport Layer Security (TLS) Internet Protocol.
B. Transport Layer Security (TLS) Data Protocol.
C. Transport Layer Security (TLS) Link Protocol.
D. Transport Layer Security (TLS) Handshake Protocol.

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 284
Similar to Secure Shell (SSH-2), Secure Sockets Layer (SSL) uses symmetric encryption for encrypting the bulk of the data being sent over the session and it uses asymmetric or public key cryptography for:

A. Peer Authentication
B. Peer Identification
C. Server Authentication
D. Name Resolution

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: SSL provides for Peer Authentication. Though peer authentication is possible, authentication of the client is seldom used in practice when connecting to public e-commerce web sites. Once authentication is complete, confidentiality is assured over the session by the use of symmetric encryption in the interests of better performance.
The following answers were all incorrect:
"Peer identification" is incorrect. The desired attribute is assurance of the identity of the communicating parties provided by authentication and NOT identification. Identification is only who you claim to be. Authentication is proving who you claim to be. "Server authentication" is incorrect. While server authentication only is common practice, the protocol provides for peer authentication (i.e., authentication of both client and server). This answer was not complete.
"Name resolution" is incorrect. Name resolution is commonly provided by the Domain Name System (DNS) not SSL.
Reference(s) used for this question:
CBK, pp. 496 - 497.

QUESTION 285
What can a packet filtering firewall also be called?

A. a scanning router
B. a shielding router
C. a sniffing router
D. a screening router

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: While neither CBK nor AIO3 use the term "screening router," they both discuss how the packet filtering capabilities of a router can be used to block traffic much like a packet filtering firewall. Krutz and Vine use this term on p. 90.
"A scanning router" is incorrect. This is a nonsense term to distract you. "A shielding router" is incorrect. This is a nonsense term to distract you. "A sniffing router" is incorrect. This is a nonsense term to distract you.

CBK, p. 433
AIO3, pp.484 - 485

QUESTION 286
Packet Filtering Firewalls examines both the source and destination address of the:

A. incoming and outgoing data packets
B. outgoing data packets only
C. Incoming Data packets only
D. user data packet

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Packeting filtering firewalls are devices that enforce administrative security policies by filtering incoming traffic as well as outgoing traffic based on rules that can include the source and/or destination addresses.
"Outgoing data packets" is incorrect. Firewalls filter incoming as well as outgoing traffic. This is sometimes called Egress and Ingress filtering.
"Incoming data packets only" is incorrect. (see previous explantion) "User data packet" is incorrect. A packet filtering firewall does not typicallly look into the data portion of the packet.
References
CBK, p. 464
AIO3, pp. 482 - 484

QUESTION 287
Packet Filtering Firewalls can also enable access for:

A. only authorized application port or service numbers.
B. only unauthorized application port or service numbers.
C. only authorized application port or ex-service numbers.
D. only authorized application port or service integers.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Firewall rules can be used to enable access for traffic to specific ports or services. "Service numbers" is rather stilted English but you may encounter these types of wordings on the actual exam -- don't let them confuse you.
"Only unauthorized application port or service numbers" is incorrect. Unauthorized ports/services would be blocked in a properly installed firewall rather than permitting access. "Only authorized application port or ex-service numbers" is incorrect. "Ex-service" numbers is a nonsense term meant to distract you.
"Only authorized application port or service integers." While service numbers are in fact integers, the more usual (and therefore better) answer is either service or "service number." References
CBK, p. 464

AIO3, pp. 482 484

QUESTION 288
A Packet Filtering Firewall system is considered a:

A. first generation firewall.
B. second generation firewall.
C. third generation firewall.
D. fourth generation firewall.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The first types of firewalls were packet filtering firewalls. It is the most basic firewall making access decisions based on ACL's. It will filter traffic based on source IP and port as well as destination IP and port. It does not understand the context of the communication and inspects every single packet one by one without understanding the context of the connection. "Second generation firewall" is incorrect. The second generation of firewall were Proxy based firewalls. Under proxy based firewall you have Application Level Proxy and also the Circuit-level proxy firewall. The application level proxy is very smart and understand the inner structure of the protocol itself. The Circui-Level Proxy is a generic proxy that allow you to proxy protocols for which you do not have an Application Level Proxy. This is better than allowing a direct connection to the net. Today a great example of this would be the SOCKS protocol. "Third generation firewall" is incorrect. The third generation firewall is the Stateful Inspection firewall. This type of firewall makes use of a state table to maintain the context of connections being established.
"Fourth generation firewall" is incorrect. The fourth generation firewall is the dynamic packet filtering firewall.

CBK, p. 464
AIO3, pp. 482 - 484
Neither CBK or AIO3 use the generation terminology for firewall types but you will encounter it frequently as a practicing security professional. See http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch3.htm for a general discussion of the different generations.

QUESTION 289
Proxies works by transferring a copy of each accepted data packet from one network to another, thereby masking the:

A. data's payload
B. data's details
C. data's owner
D. data's origin

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The application firewall (proxy) relays the traffic from a trusted host running a specific application to an untrusted server. It will appear to the untrusted server as if the request originated from the proxy server. "Data's payload" is incorrect. Only the origin is changed. "Data's details" is incorrect. Only the origin is changed. "Data's owner" is incorrect. Only the origin is changed.

CBK, p. 467
AIO3, pp. 486 - 490

QUESTION 290
A proxy can control which services (FTP and so on) are used by a workstation , and also aids in protecting the

network from outsiders who may be trying to get information about the:

A. network's design
B. user base
C. operating system design
D. net BIOS' design

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: To the untrusted host, all traffic seems to originate from the proxy server and addresses on the trusted network are not revealed.
"User base" is incorrect. The proxy hides the origin of the request from the untrusted host. "Operating system design" is incorrect. The proxy hides the origin of the request from the untrusted host.
"Net BIOS' design" is incorrect. The proxy hides the origin of the request from the untrusted host.

CBK, p. 467
AIO3, pp. 486 - 490

QUESTION 291
A proxy is considered a:

A. first generation firewall.
B. third generation firewall.
C. second generation firewall.
D. fourth generation firewall.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The proxy (application layer firewall, circuit level proxy, or application proxy) is a second generation firewall
"First generation firewall" incorrect. A packet filtering firewall is a first generation firewall. "Third generation firewall" is incorrect. Stateful Firewall are considered third generation firewalls "Fourth generation firewall" is incorrect. Dynamic packet filtering firewalls are fourth generation firewalls

CBK, p. 464
AIO3, pp. 482 - 484
Neither CBK or AIO3 use the generation terminology for firewall types but you will encounter it frequently as a practicing security professional. See http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch3.htm for a general discussion of the different generations.

QUESTION 292
An application layer firewall is also called a:

A. Proxy
B. A Presentation Layer Gateway.
C. A Session Layer Gateway.
D. A Transport Layer Gateway.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: An application layer firewall can also be called a proxy. "A presentation layer gateway" is incorrect. A gateway connects two unlike environments and is usually required to translate between diffferent types of applications or protocols. This is not the function of a firewall.
"A session layer gateway" is incorrect. A gateway connects two unlike environments and is usually required to translate between diffferent types of applications or protocols. This is not the function of a firewall.
"A transport layer gateway" is incorrect. A gateway connects two unlike environments and is usually required to translate between diffferent types of applications or protocols. This is not the function of a firewall.

CBK, p. 467
AIO3, pp. 486 - 490, 960

QUESTION 293
Application Layer Firewalls operate at the:

A. OSI protocol Layer seven, the Application Layer.
B. OSI protocol Layer six, the Presentation Layer.
C. OSI protocol Layer five, the Session Layer.
D. OSI protocol Layer four, the Transport Layer.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Since the application layer firewall makes decisions based on application-layer information in the packet, it operates at the application layer of the OSI stack. "OSI protocol layer 6, the presentation layer" is incorrect. The application layer firewall must have access to the application layer information in the packet and therefore operates at the application layer.
"OSI protocol layer 5, the session layer" is incorrect. The application layer firewall must have access to the application layer information in the packet and therefore operates at the application layer.
"OSI protocol layer 4, the transport layer" is incorrect. The application layer firewall must have access to the application layer information in the packet and therefore operates at the application layer.

CBK, p. 467
AIO3, pp.488 - 490

QUESTION 294
A variation of the application layer firewall is called a:

A. Current Level Firewall.
B. Cache Level Firewall.
C. Session Level Firewall.
D. Circuit Level Firewall.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Terminology can be confusing between the different souces as both CBK and AIO3 call an application layer firewall a proxy and proxy servers are generally classified as either circuitlevel proxies or application level proxies.
The distinction is that a circuit level proxy creates a conduit through which a trusted host can communicate with an untrusted one and doesn't really look at the application contents of the packet (as an application level proxy does). SOCKS is one of the better known circuit-level proxies.
Firewalls
Packet Filtering Firewall - First Generation
n Screening Router

n Operates at Network and Transport level
n Examines Source and Destination IP Address
n Can deny based on ACLs
n Can specify Port
Application Level Firewall - Second Generation
n Proxy Server
n Copies each packet from one network to the other
n Masks the origin of the data
n Operates at layer 7 (Application Layer)
n Reduces Network performance since it has do analyze each packet and decide what to do with it.
n Also Called Application Layer Gateway
Stateful Inspection Firewalls Third Generation
n Packets Analyzed at all OSI layers
n Queued at the network level
n Faster than Application level Gateway
Dynamic Packet Filtering Firewalls Fourth Generation n Allows modification of security rules
n Mostly used for UDP
n Remembers all of the UDP packets that have crossed the network's perimeter, and it decides whether to enable packets to pass through the firewall.
Kernel Proxy Fifth Generation
n Runs in NT Kernel
n Uses dynamic and custom TCP/IP-based stacks to inspect the network packets and to enforce security policies.
"Current level firewall" is incorrect. This is an amost-right-sounding distractor to confuse the unwary.
"Cache level firewall" is incorrect. This too is a distractor. "Session level firewall" is incorrect. This too is a distractor.
References
CBK, p. 466 - 467
AIO3, pp. 486 - 490
CISSP Study Notes from Exam Prep Guide

QUESTION 295
A circuit level proxy is when compared to an application level proxy.

A. lower in processing overhead.
B. more difficult to maintain.
C. more secure.
D. slower.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Since the circuit level proxy does not anayze the application content of the packet in making its decisions, it has lower overhead than an application level proxy. "More difficult to maintain" is incorrect. Circuit level proxies are typicall easier to configure and simpler to maintain that an application level proxy.
"More secure" is incorrect. A circuit level proxy is not necessarily more secure than an application layer proxy.
"Slower" is incorrect. Because it is lower in overhead, a circuit level proxy is typically faster than an application level proxy.

CBK,pp. 466 - 467
AIO3, pp.488 - 490

QUESTION 296
In a stateful inspection firewall, data packets are captured by an inspection engine that is operating at the:

A. Network or Transport Layer.
B. Application Layer.

C. Inspection Layer.

D. Data Link Layer.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Most stateful packet inspection firewalls work at the network or transport layers. For the TCP/IP protcol, this allows the firewall to make decisions both on IP addresses, protocols and TCP/UDP port numbers Application layer is incorrect. This is too high in the OSI stack for this type of firewall. Inspection layer is incorrect. There is no such layer in the OSI stack. "Data link layer" is incorrect. This is too low in the OSI stack for this type of firewall.

CBK, p. 466
AIO3, pp. 485 - 486

QUESTION 297
In stateful inspection firewalls, packets are:

A. Inspected at only one layer of the Open System Interconnection (OSI) model

B. Inspected at all Open System Interconnection (OSI) layers

C. Decapsulated at all Open Systems Interconnect (OSI) layers.

D. Encapsulated at all Open Systems Interconnect (OSI) layers.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Many times when a connection is opened, the firewall will inspect all layers of the packet. While this inspection is scaled back for subsequent packets to improve performance, this is the best of the four answers.
When packet filtering is used, a packet arrives at the firewall, and it runs through its ACLs to determine whether this packet should be allowed or denied. If the packet is allowed, it is passed on to the destination host, or to another network device, and the packet filtering device forgets about the packet. This is different from stateful inspection, which remembers and keeps track of what packets went where until each particular connection is closed. A stateful firewall is like a nosy neighbor who gets into people's business and conversations. She keeps track of the suspicious cars that come into the neighborhood, who is out of town for the week, and the postman who stays a little too long at the neighbor lady's house. This can be annoying until your house is burglarized. Then you and the police will want to talk to the nosy neighbor, because she knows everything going on in the neighborhood and would be the one most likely to know something unusual happened.
"Inspected at only one Open Systems Interconnetion (OSI) layer" is incorrect. To perform stateful packet inspection, the firewall must consider at least the network and transport layers. "Decapsulated at all Open Systems Interconnection (OSI) layers" is incorrect. The headers are not stripped ("decapsulated" if there is such a word) and are passed through in their entirety IF the packet is passed.
"Encapsulated at all Open Systems Interconnect (OSI) layers" is incorrect. Encapsulation refers to the adding of a layer's header/trailer to the information received from the above level. This is done when the packet is assembled not at the firewall.
Reference(s) used for this question:
CBK, p. 466
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (pp. 632-633). McGraw-Hill. Kindle Edition.

QUESTION 298
When an outgoing request is made on a port number greater than 1023, this type of firewall creates an ACL to allow the incoming reply on that port to pass:

A. packet filtering
B. CIrcuit level proxy
C. Dynamic packet filtering
D. Application level proxy

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The dynamic packet filtering firewall is able to create ACL's on the fly to allow replies on dynamic ports (higher than 1023).
Packet filtering is incorrect. The packet filtering firewall usually requires that the dynamic ports be left open as a group in order to handle this situiation. Circuit level proxy is incorrect. The circuit level proxy builds a conduit between the trusted and untrusted hosts and does not work by dynamically creating ACL's. Application level proxy is incorrect. The application level proxy "proxies" for the trusted host in its communications with the untrusted host. It does not dynamically create ACL's to control traffic.

QUESTION 299
The general philosophy for DMZ's is that:

A. any system on the DMZ can be compromized because it's accessible from the Internet.
B. any system on the DMZ cannot be compromized because it's not accessible from the Internet.
C. some systems on the DMZ can be compromized because they are accessible from the Internet.
D. any system on the DMZ cannot be compromized because it's by definition 100 percent safe and not accessible from the Internet.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Because the DMZ systems are accessible from the Internet, they are more at risk for attacka nd compromise and must be hardened appropriately. "Any system on the DMZ cannot be compromised because it's not accessible from the Internet" is incorrect. The reason a system is placed in the DMZ is so it can be accessible from the Internet. "Some systems on the DMZ can be compromised because they are accessible from the Internet" is incorrect. All systems in the DMZ face an increased risk of attack and compromise because they are accessible from the Internet.
"Any system on the DMZ cannot be compromised because it's by definition 100 percent safe and not accessible from the Internet" is incorrect. Again, a system is placed in the DMZ because it must be accessible from the Internet.

CBK, p. 434
AIO3, p. 483

QUESTION 300
A DMZ is located:

A. right behind your first Internet facing firewall
B. right in front of your first Internet facing firewall
C. right behind your first network active firewall
D. right behind your first network passive Internet http firewall

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: While the purpose of systems in the DMZ is to allow public access to certain internal network

resources (EMAIL, DNS, Web), it is a good practice to restrict that access to the minimum necessary to provide those services through use of a firewall. In computer security, a DMZ or Demilitarized Zone (sometimes referred to as a perimeter network) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external attacker only has direct access to equipment in the DMZ, rather than any other part of the network. The name is derived from the term "demilitarized zone", an area between nation states in which military operation is not permitted.
The following are incorrect answers:
"Right in front of your first Internet facing firewall" While the purpose of systems in the DMZ is to allow public access to certain internal network resources (EMAIL, DNS, Web), it is a good practice to restrict that access to the minimum necessary to provide those services through use of a firewall.
"Right behind your first network active firewall" This is an almost-right-sounding answer meant to distract the unwary.
"Right behind your first network passive Internet http firewall" This is an almost-right-sounding answer meant to distract the unwary.

CBK, p. 434
and
AIO3, p. 483
and
http://en.wikipedia.org/wiki/DMZ_%28computing%29

QUESTION 301
Good security is built on which of the following concept?

A. The concept of a pass-through device that only allows certain traffic in and out

B. The Concept of defense in depth

C. The Concept of Preventative controls

D. The Concept of Defensive Controls

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: This the best of the four answers as a defense that depends on multiple layers is superior to one where all protection is embedded in a single layer (e.g., a firewall). Defense in depth would include all categories of controls.
The Following answers are incorrect:
"Concept of a pass through device that only allows certain traffic in and out" is incorrect. This is one definition of a firewall which can be a component of a defense in depth strategy in combination with other measures.
"Concept of preventative controls" is incorrect. This is a component of a defense in depth strategy but the core concept is that there must be multiple layers of defenses. "Concept of defensive controls" is incorrect. This is a component of a defense in depth strategy but the core concept is that there must be multiple layers of defenses.

http://en.wikipedia.org/wiki/Defense_in_depth_(computing) http://www.nsa.gov/snac/support/defenseindepth.pdf

QUESTION 302
A DMZ is also known as a

A. screened subnet

B. three legged firewall

C. a place to attract hackers

D. bastion host

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: This is another name for the demilitarized zone (DMZ) of a network. "Three legged firewall" is incorrect. While a DMZ can be implemented on one leg of such a device, this is not the best answer.
"A place to attract hackers" is incorrect. The DMZ is a way to provide limited public access to an organization's internal resources (DNS, EMAIL, public web, etc) not as an attractant for hackers. "Bastion host" is incorrect. A bastion host serves as a gateway between trusted and untrusted network.

CBK, p. 434
AIO3, pp. 495 - 496

QUESTION 303
Which of the following would be used to detect and correct errors so that integrity and confidentiality of transactions over networks may be maintained while preventing unauthorize interception of the traffic?

A. Information security
B. Server security
C. Client security
D. Communications security

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Communications security is the discipline of preventing unauthorized interceptors from accessing telecommunications in an intelligible form, while still delivering content to the intended recipients. In the United States Department of Defense culture, it is often referred to by the abbreviation COMSEC. The field includes cryptosecurity, transmission security, emission security, traffic-flow security and physical security of COMSEC equipment.
All of the other answers are incorrect answers:
Information security
Information security would be the overall program but communications security is the more specific and better answer. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.
The terms information security, computer security and information assurance are frequently incorrectly used interchangeably. These fields are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them.
These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms. Computer security can focus on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer.
Server security
While server security plays a part in the overall information security program, communications security is a better answer when talking about data over the network and preventing interception. See publication 800-123 listed in the reference below to learn more.
Client security
While client security plays a part in the overall information security program, communications security is a better answer. Securing the client would not prevent interception of data or capture of data over the network. Today people referred to this as endpoint security.

http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf and
https://en.wikipedia.org/wiki/Information_security
and
https://en.wikipedia.org/wiki/Communications_security

QUESTION 304
Which of the following prevents, detects, and corrects errors so that the integrity, availability, and confidentiality of transactions over networks may be maintained?

A. Communications security management and techniques
B. Information security management and techniques
C. Client security management and techniques
D. Server security management and techniques

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Communications security and techniques are the best area for addressing this objective. "Information security management and techniques" is incorrect. While the overall information security program would include this objective, communications security is the more specific and better answer. "Client security management and techniques" is incorrect. While client security plays a part in this overall objective, communications security is the more specific and better answer. "Server security management and techniques" is incorrect. While server security plays a part in this overall objective, communications security is the more specific and better answer.

CBK, p. 408

QUESTION 305
The Telecommunications Security Domain of information security is also concerned with the prevention and detection of the misuse or abuse of systems, which poses a threat to the tenets of:

A. Confidentiality, Integrity, and Entity (C.I.E.).
B. Confidentiality, Integrity, and Authenticity (C.I.A.).
C. Confidentiality, Integrity, and Availability (C.I.A.).
D. Confidentiality, Integrity, and Liability (C.I.L.).

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The CIA acronym stands for Confidentiality, Integrity and Availability. "Confidentiality, Integrity and Entity (CIE)" is incorrect. "Entity" is not part of the telecommunications domain definition. "Confidentiality, Integrity and Authenticity (CIA)" is incorrect. While authenticity is included in the telecommunications domain, CIA is the acronym for confidentiality, integrity and availability. "Confidentiality, Integrity, and Liability (CIL)" is incorrect. Liability is not part of the telecommunications domain definition.

CBK, pp. 407 - 408

QUESTION 306
Which of the following elements of telecommunications is not used in assuring confidentiality?

A. Network security protocols
B. Network authentication services
C. Data encryption services
D. Passwords

Correct Answer: D
Explanation

Explanation/Reference:

Explanation: Passwords are one of the multiple ways to authenticate (prove who you claim to be) an identity which allows confidentiality controls to be enforced to assure the identity can only access the information for which it is authorized. It is the authentication that assists assurance of confidentiality not the passwords.

"Network security protocols" is incorrect. Network security protocols are quite useful in assuring confidentiality in network communications.

"Network authentication services" is incorrect. Confidentiality is concerned with allowing only authorized users to access information. An important part of determining authorization is authenticating an identity and this service is supplied by network authentication services. "Data encryption services" is incorrect. Data encryption services are quite useful in protecting the confidentiality of information.

Reference(s) used for this question:

Official ISC2 Guide to the CISSP CBK, pp. 407 - 520

AIO 3rd Edition, pp. 415 - 580

QUESTION 307

Which cable technology refers to the CAT3 and CAT5 categories?

A. Coaxial cables

B. Fiber Optic cables

C. Axial cables

D. Twisted Pair cables

Correct Answer: D

Explanation

Explanation/Reference:

Explanation: Twisted Pair cables currently have two categories in common usage. CAT3 and CAT5.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 72.

QUESTION 308

Which of the following was designed as a more fault-tolerant topology than Ethernet, and very resilient when properly implemented?

A. Token Link.

B. Token system.

C. Token Ring.

D. Duplicate ring.

Correct Answer: C

Explanation

Explanation/Reference:

Explanation: Token Ring was designed to be a more fault-tolerant topology than Ethernet, and can be a very resilient topology when properly implemented. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 72.

QUESTION 309

Which of the following is a token-passing scheme like token ring that also has a second ring that remains dormant until an error condition is detected on the primary ring?

A. Fiber Distributed Data Interface (FDDI).

B. Ethernet

C. Fast Ethernet

D. Broadband

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: FDDI is a token-passing ring scheme like a token ring, yet it also has a second ring that remains dormant until an error condition is detected on the primary ring. Fiber Distributed Data Interface (FDDI) provides a 100 Mbit/s optical standard for data transmission in a local area network that can extend in range up to 200 kilometers (124 miles). Although FDDI logical topology is a ring-based token network, it does not use the IEEE 802.5 token ring protocol as its basis; instead, its protocol is derived from the IEEE 802.4 token bus timed token protocol. In addition to covering large geographical areas, FDDI local area networks can support thousands of users. As a standard underlying medium it uses optical fiber, although it can use copper cable, in which case it may be refer to as CDDI (Copper Distributed Data Interface). FDDI offers both a Dual-Attached Station (DAS), counter-rotating token ring topology and a Single-Attached Station (SAS), token bus passing ring topology. Ethernet is a family of frame-based computer networking technologies for local area networks (LANs). The name came from the physical concept of the ether. It defines a number of wiring and signaling standards for the Physical Layer of the OSI networking model as well as a common addressing format and Media Access Control at the Data Link Layer. In computer networking, Fast Ethernet is a collective term for a number of Ethernet standards that carry traffic at the nominal rate of 100 Mbit/s, against the original Ethernet speed of 10 Mbit/s. Of the fast Ethernet standards 100BASE-TX is by far the most common and is supported by the vast majority of Ethernet hardware currently produced. Fast Ethernet was introduced in 1995 and remained the fastest version of Ethernet for three years before being superseded by gigabit Ethernet.
Broadband in data can refer to broadband networks or broadband Internet and may have the same meaning as above, so that data transmission over a fiber optic cable would be referred to as broadband as compared to a telephone modem operating at 56,000 bits per second. However, a worldwide standard for what level of bandwidth and network speeds actually constitute Broadband have not been determined.[1]
Broadband in data communications is frequently used in a more technical sense to refer to data transmission where multiple pieces of data are sent simultaneously to increase the effective rate of transmission, regardless of data signaling rate. In network engineering this term is used for methods where two or more signals share a medium.[Broadband Internet access, often shortened to just broadband, is a high data rate Internet access--typically contrasted with dial-up access using a 56k modem.
Dial-up modems are limited to a bitrate of less than 56 kbit/s (kilobits per second) and require the full use of a telephone line--whereas broadband technologies supply more than double this rate and generally without disrupting telephone use.
Source:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 72.
also see:
http://en.wikipedia.org/

QUESTION 310
A common way to create fault tolerance with leased lines is to group several T1s together with an inverse multiplexer placed:

A. at one end of the connection.
B. at both ends of the connection.
C. somewhere between both end points.
D. in the middle of the connection.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: A common way to create fault tolerance with leased lines is to group several T1s together with an inverse multiplexer placed at both ends of the connection. In fact it would be a Multiplexer at one end and DeMultiplexer at other end or vice versa. Inverse Multiplexer at both end.
In electronics, a multiplexer (or mux) is a device that selects one of several analog or digital input signals and forwards the selected input into a single line. A multiplexer of 2n inputs has n select lines, which are used to select which input line to send to the output. Multiplexers are mainly used to increase the amount of data that

can be sent over the network within a certain amount of time and bandwidth. A multiplexer is also called a data selector. An electronic multiplexer makes it possible for several signals to share one device or resource, for example one A/D converter or one communication line, instead of having one device per input signal.
On the other hand, a demultiplexer (or demux) is a device taking a single input signal and selecting one of many data-output-lines, which is connected to the single input. A multiplexer is often used with a complementary demultiplexer on the receiving end. An electronic multiplexer can be considered as a multiple-input, single-output switch, and a demultiplexer as a single-input, multiple-output switch

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 72.
and
https://secure.wikimedia.org/wikipedia/en/wiki/Multiplexer

QUESTION 311
Frame relay uses a public switched network to provide:

A. Local Area Network (LAN) connectivity.
B. Metropolitan Area Network (MAN) connectivity.
C. Wide Area Network (WAN) connectivity.
D. World Area Network (WAN) connectivity.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Frame relay uses a public switched network to provide Wide Area Network (WAN) connectivity.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 73.

QUESTION 312
What is a TFTP server most useful for?

A. Transferring configurations to and from network devices.
B. Transferring files to web servers.
C. Terminal access to network devices.
D. Terminal access to file servers.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: A Trivial File Transfer Protocol (TFTP) server can be used when configuring network devices to transfer configurations to and from network devices. Many networking devices now support TFTP.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 73).

QUESTION 313
Which type of attack consists of modifying the length and fragmentation offset fields in sequential IP packets?

A. Teardrop attack
B. Smurf attack
C. SYN attack
D. Buffer overflow attack

Correct Answer: A

Explanation

Explanation/Reference:
Explanation: A teardrop attack consists of modifying the length and fragmentation offset fields in sequential IP packets so the target system becomes confused and crashes after it receives contradictory instructions on how the fragments are offset on these packets. A SYN attack is when an attacker floods a system with connection requests but does not respond when the target system replies to those requests. A smurf attack is an attack where the attacker spoofs the source IP address in an ICMP ECHO broadcast packet so it seems to have originated at the victim's system, in order to flood it with REPLY packets. A buffer overflow attack occurs when a process receives much more data than expected.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 76).

QUESTION 314
What is called an attack in which an attacker floods a system with connection requests but does not respond when the target system replies to those requests?

A. Ping of death attack
B. SYN attack
C. Smurf attack
D. Buffer overflow attack

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: A SYN attack occurs when an attacker floods the target system's small "in-process" queue with connection requests, but it does not respond when the target system replies to those requests. This causes the target system to "time out" while waiting for the proper response, which makes the system crash or become unusable. A buffer overflow attack occurs when a process receives much more data than expected. One common buffer overflow attack is the ping of death, where an attacker sends IP packets that exceed the maximum legal length (65535 octets). A smurf attack is an attack where the attacker spoofs the source IP address in an ICMP ECHO broadcast packet so it seems to have originated at the victim's system, in order to flood it with REPLY packets.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 76).

QUESTION 315
What type of attack involves IP spoofing, ICMP ECHO and a bounce site?

A. IP spoofing attack
B. Teardrop attack
C. SYN attack
D. Smurf attack

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: A smurf attack occurs when an attacker sends a spoofed (IP spoofing) PING (ICMP ECHO) packet to the broadcast address of a large network (the bounce site). The modified packet containing the address of the target system, all devices on its local network respond with a ICMP REPLY to the target system, which is then saturated with those replies. An IP spoofing attack is used to convince a system that it is communication with a known entity that gives an intruder access. It involves modifying the source address of a packet for a trusted source's address. A teardrop attack consists of modifying the length and fragmentation

offset fields in sequential IP packets so the target system becomes confused and crashes after it receives contradictory instructions on how the fragments are offset on these packets. A SYN attack is when an attacker floods a system with connection requests but does not respond when the target system replies to those requests.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 76).

QUESTION 316
Which type of attack involves the alteration of a packet at the IP level to convince a system that it is communicating with a known entity in order to gain access to a system?

A. TCP sequence number attack
B. IP spoofing attack
C. Piggybacking attack
D. Teardrop attack

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: An IP spoofing attack is used to convince a system that it is communication with a known entity that gives an intruder access. It involves modifying the source address of a packet for a trusted source's address. A TCP sequence number attack involves hijacking a session between a host and a target by predicting the target's choice of an initial TCP sequence number. Piggybacking refers to an attacker gaining unauthorized access to a system by using a legitimate user's connection. A teardrop attack consists of modifying the length and fragmentation offset fields in sequential IP packets so the target system becomes confused and crashes after it receives contradictory instructions on how the fragments are offset on these packets. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 77).

QUESTION 317
Which type of attack involves hijacking a session between a host and a target by predicting the target's choice of an initial TCP sequence number?

A. IP spoofing attack
B. SYN flood attack
C. TCP sequence number attack
D. Smurf attack

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: A TCP sequence number attack exploits the communication session which was established between the target and the trusted host that initiated the session. It involves hijacking the session between the host and the target by predicting the target's choice of an initial TCP sequence number. An IP spoofing attack is used to convince a system that it is communication with a known entity that gives an intruder access. It involves modifying the source address of a packet for a trusted source's address. A SYN attack is when an attacker floods a system with connection requests but does not respond when the target system replies to those requests. A smurf attack occurs when an attacker sends a spoofed (IP spoofing) PING (ICMP ECHO) packet to the broadcast address of a large network (the bounce site). The modified packet containing the address of the target system, all devices on its local network respond with a ICMP REPLY to the target system, which is then saturated with those replies. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 77).

QUESTION 318
Which layer defines how packets are routed between end systems?

A. Session layer
B. Transport layer
C. Network layer
D. Data link layer

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The network layer (layer 3) defines how packets are routed and relayed between end systems on the same network or on interconnected networks. Message routing, error detection and control of node traffic are managed at this level.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 82).

QUESTION 319
Which OSI/ISO layers are TCP and UDP implemented at?

A. Application layer
B. Presentation layer
C. Session layer
D. Transport layer

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: TCP and UDP are implemented at the transport layer (layer 4). Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 82).

QUESTION 320
Which ISO/OSI layer establishes the communications link between individual devices over a physical link or channel?

A. Transport layer
B. Network layer
C. Data link layer
D. Physical layer

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The data link layer (layer 2) establishes the communications link between individual devices over a physical link or channel. It also ensures that messages are delivered to the proper device and translates the messages from layers above into bits for the physical layer (layer 1) to transmit.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 83).

QUESTION 321
Which OSI/ISO layer is the Media Access Control (MAC) sublayer part of?

A. Transport layer
B. Network layer
C. Data link layer
D. Physical layer

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The data link layer contains the Logical Link Control sublayer and the Media Access Control (MAC) sublayer.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 83).

QUESTION 322
How many layers are defined within the US Department of Defense (DoD) TCP/IP Model?

A. 7
B. 5
C. 4
D. 3

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The TCP/IP protocol model is similar to the OSI model but it defines only four layers:
Application
Host-to-host
Internet
Network access
Reference(s) used for this question:
http://www.novell.com/documentation/nw65/ntwk_ipv4_nw/data/hozdx4oj.html and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 84).
also see:
http://en.wikipedia.org/wiki/Internet_Protocol_Suite#Layer_names_and_number_of_layers_in_the _literature

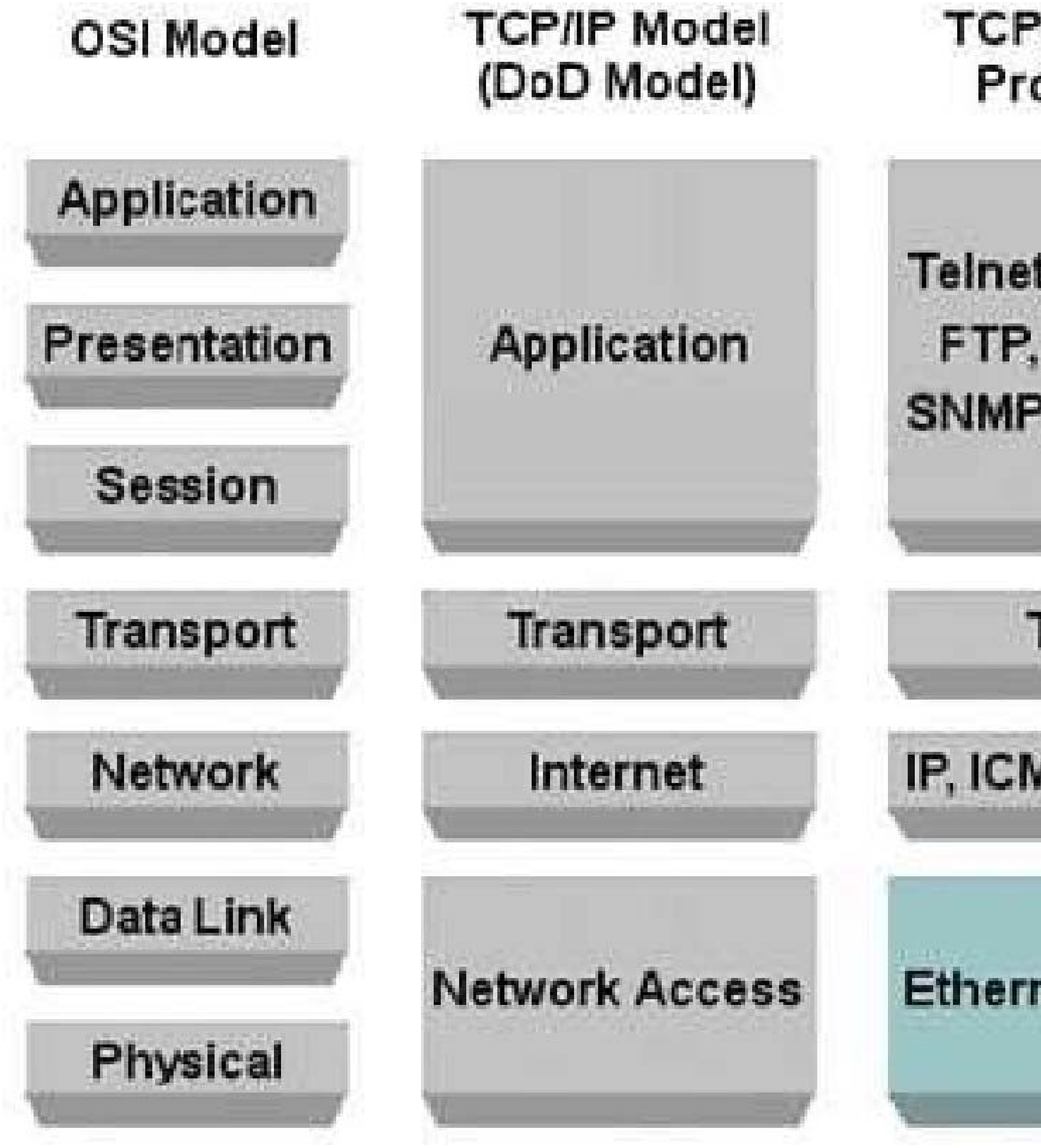
QUESTION 323
As per RFC 1122, which of the following is not a defined layer in the DoD TCP/IP protocol model?

A. Application layer
B. Session layer
C. Internet layer
D. Link/Network Access Layer

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: As per RFC, The DoD TCP/IP protocol model defines four layers, with the layers having names, not numbers, as follows:

Application (process-to-process) Layer:
This is the scope within which applications create user data and communicate this data to other processes or applications on another or the same host. The communications partners are often called peers. This is where the "higher level" protocols such as SMTP, FTP, SSH, HTTP, etc.
operate.
Transport (host-to-host) Layer:
The Transport Layer constitutes the networking regime between two network hosts, either on the local network or on remote networks separated by routers. The Transport Layer provides a uniform networking interface that hides the actual topology (layout) of the underlying network connections. This is where flow-control, error-correction, and connection protocols exist, such as TCP. This layer deals with opening and maintaining connections between internet hosts.
Internet (internetworking) Layer:
The Internet Layer has the task of exchanging datagrams across network boundaries. It is therefore also referred to as the layer that establishes internetworking; indeed, it defines and establishes the Internet. This layer defines the addressing and routing structures used for the TCP/IP protocol suite. The primary protocol in this scope is the Internet Protocol, which defines IP addresses. Its function in routing is to transport datagrams to the next IP router that has the connectivity to a network closer to the final data destination.
Link (network access) Layer:
This layer defines the networking methods with the scope of the local network link on which hosts communicate without intervening routers. This layer describes the protocols used to describe the local network topology and the interfaces needed to affect transmission of Internet Layer datagrams to next-neighbor hosts.
The DoD tcp/ip model DoD model Osi Model



Graphic above from: http://bit.kuas.edu.tw/
REALITY VERSUS THE STANDARD
In real life today, this is getting very confusing. Many books and references will not use exactly the same names as the initial RFC that was published. For example, the Link layer is often times called Network Access.

The same applies with Transport which is often times called Host-to-Host and vice versa.
The following answer is incorrect:
The session layer is defined within the OSI/ISO model but not within the DOD model. Being incorrect it made it the best answer according to the question. It does not belong to the DoD TCP/IP Model.
Reference(s) Used for this question:
http://www.freesoft.org/CIE/RFC/1122/
http://bit.kuas.edu.tw/~csshieh/teach/np/tcpip/

QUESTION 324
Which layer of the DoD TCP/IP Model ensures error-free delivery and packet sequencing?

A. Internet layer
B. Network access layer
C. Host-to-host
D. Application layer

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: This layer of the DoD Model is also sometimes called Transport in some books but the proper name is Host-to-Host as per the RFC document. The host-to-host layer provides for reliable end-to-end communications, ensures the data's errorfree delivery, handles the data's packet sequencing, and maintains the data's integrity. It is comparable to the transport layer of the OSI model.
Reference(s) used for this question:
http://en.wikipedia.org/wiki/Internet_protocol_suite
and
http://technet.microsoft.com/en-us/library/cc786900%28v=ws.10%29.aspx and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 85).

QUESTION 325
Which layer of the TCP/IP protocol model would best correspond to the OSI/ISO model's network layer?

A. Network access layer
B. Application layer
C. Host-to-host transport layer
D. Internet layer

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The Internet layer corresponds to the OSI's network layer. It handles the routing of packets among multiple networks.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 85).

QUESTION 326
Which layer of the DoD TCP/IP model controls the communication flow between hosts?

A. Internet layer
B. Host-to-host transport layer
C. Application layer
D. Network access layer

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Whereas the host-to-host layer (equivalent to the OSI's transport layer) provides end-to-end data delivery service, flow control, to the application layer. The four layers in the DoD model, from top to bottom, are:
The Application Layer contains protocols that implement user-level functions, such as mail delivery, file transfer and remote login.
The Host-to-Host Layer handles connection rendez vous, flow control, retransmission of lost data, and other generic data flow management between hosts. The mutually exclusive TCP and UDP protocols are this layer's most important members.
The Internet Layer is responsible for delivering data across a series of different physical networks that interconnect a source and destination machine. Routing protocols are most closely associated with this layer, as is the IP Protocol, the Internet's fundamental protocol. The Network Access Layer is responsible for delivering data over the particular hardware media in use. Different protocols are selected from this layer, depending on the type of physical network The OSI model organizes communication services into seven groups called layers. The layers are as follows:
Layer 7, The Application Layer: The application layer serves as a window for users and application processes to access network services. It handles issues such as network transparency, resource allocation, etc. This layer is not an application in itself, although some applications may perform application layer functions.
Layer 6, The Presentation Layer: The presentation layer serves as the data translator for a network. It is usually a part of an operating system and converts incoming and outgoing data from one presentation format to another. This layer is also known as syntax layer. Layer 5, The Session Layer: The session layer establishes a communication session between processes running on different communication entities in a network and can support a messagemode data transfer. It deals with session and connection coordination.
Layer 4, The Transport Layer: The transport layer ensures that messages are delivered in the order in which they are sent and that there is no loss or duplication. It ensures complete data transfer. This layer provides an additional connection below the Session layer and assists with managing some data flow control between hosts. Data is divided into packets on the sending node, and the receiving node's Transport layer reassembles the message from packets. This layer is also responsible for error checking to guarantee error-free data delivery, and requests a retransmission if necessary. It is also responsible for sending acknowledgments of successful transmissions back to the sending host. A number of protocols run at the Transport layer, including TCP, UDP, Sequenced Packet Exchange (SPX), and NWLink. Layer 3, The Network Layer: The network layer controls the operation of the subnet. It determines the physical path that data takes on the basis of network conditions, priority of service, and other factors. The network layer is responsible for routing and forwarding data packets. Layer 2, The Data-Link Layer: The data-link layer is responsible for error free transfer of data frames. This layer provides synchronization for the physical layer. ARP and RARP would be found at this layer.
Layer 1, The Physical Layer: The physical layer is responsible for packaging and transmitting data on the physical media. This layer conveys the bit stream through a network at the electrical and mechanical level.
See a great flash animation on the subject at:
http://www.maris.com/content/applets/flash/comp/fa0301.swf Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 85).
Also: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 7: Telecommunications and Network Security (page 344).

QUESTION 327
Which of the following protocols is not implemented at the Internet layer of the TCP/IP protocol model?

A. User datagram protocol (UDP)
B. Internet protocol (IP)
C. Internet Group Management Protocol (IGMP)
D. Internet control message protocol (ICMP)

Correct Answer: A
Explanation

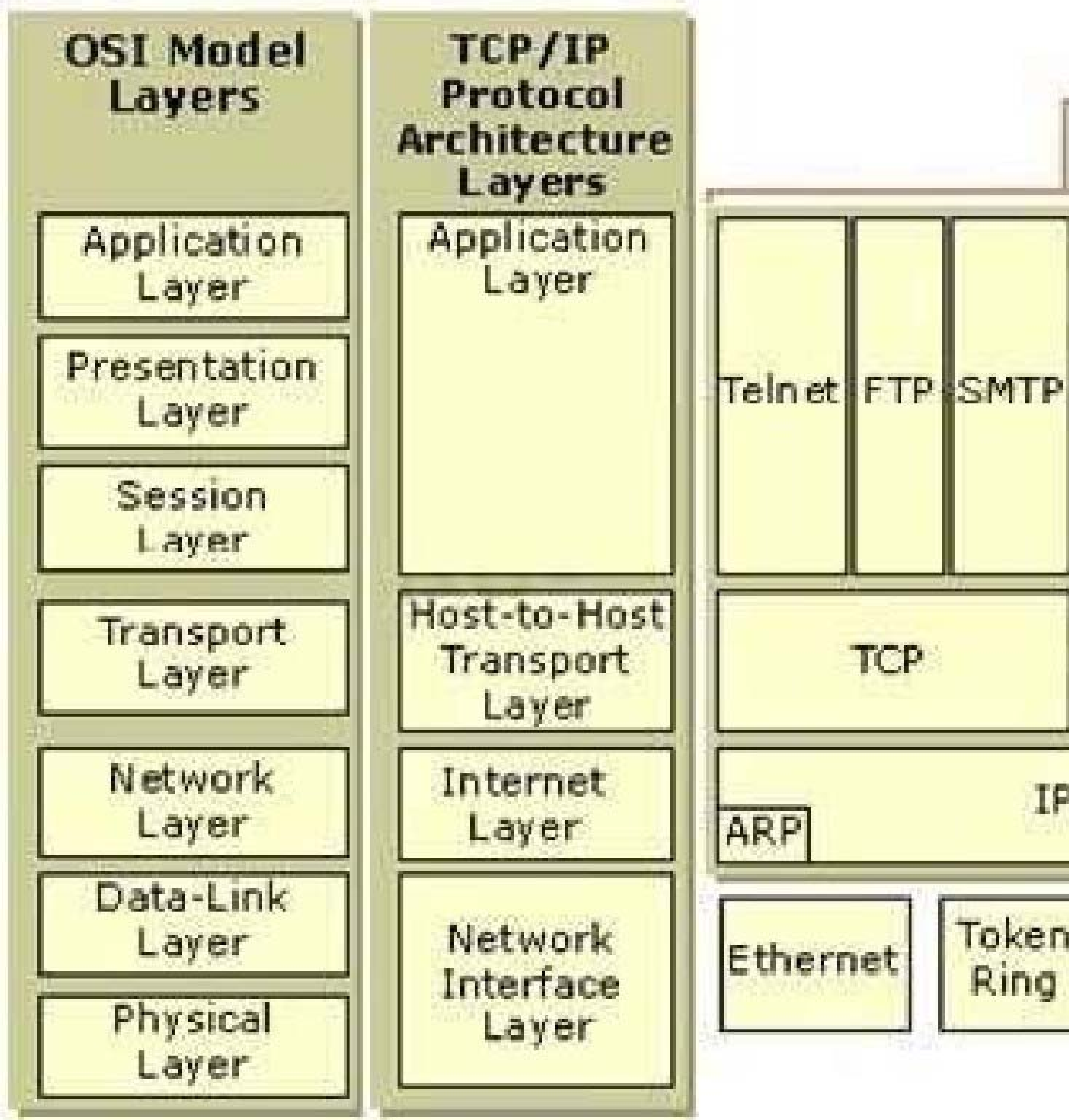
Explanation/Reference:

Explanation: The User Datagram Protocol (UDP) is implemented at the host-to-host transport layer, not at the internet layer.

Protocol at what layer?

Ensure you are familiar with both the OSI model and the DoD TCP/IP model as well. You need to know how to contrast the two side by side and what are the names being used on both side. Below you have a graphic showing the two and how things maps between the two as well as some of the most common protcolos found at each of the layers:

Protocols at what layers of the DoD TCP/IP model



Graphic from http://technet.microsoft.com/en-us/library/cc958821.aspx The following are incorrect answers:
All of the other protocols sit at the Internet Layer of the TCP/IP model.
NOTE:
Some reference are calling the Transport layer on the DoD model Host-to-Host.
Reference(s) used for this question:
Shon Harris, CISSP All In One (AIO), 6th edition , Telecommunication and Network Security, Page 518,534
and

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 85).
and
Microsoft Technet at http://technet.microsoft.com/en-us/library/cc958821.aspx

QUESTION 328
Which protocol of the TCP/IP suite addresses reliable data transport?

A. Transmission control protocol (TCP)
B. User datagram protocol (UDP)
C. Internet protocol (IP)
D. Internet control message protocol (ICMP)

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: TCP provides a full-duplex, connection-oriented, reliable, virtual circuit. It handles the sequencing and retransmission of lost packets.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 85).

QUESTION 329
Which of the following is an advantage that UDP has over TCP?

A. UDP is connection-oriented whereas TCP is not.
B. UDP is more reliable than TCP.
C. UDP is faster than TCP.
D. UDP makes a better effort to deliver packets.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: UDP is a scaled-down version of TCP. It is used like TCP, but only offers a "best effort" delivery. It is connectionless, does not offer error correction, does not sequence the packet segments, and less reliable than TCP but because of its lower overhead, it provides a faster transmission than TCP.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 86).

QUESTION 330
What protocol is used to match an IP address to the appropriate hardware address of the packet's destination so it can be sent?

A. Routing tables
B. Address resolution protocol (ARP)
C. Reverse address resolution protocol (RARP)
D. Internet Control Message Protocol (ICMP)

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The Address Resolution Protocol (ARP) is used to match an IP address to an Ethernet address

so the packet can be sent to the appropriate node.
Shon Harris in her book says:
MAC and IP addresses must be properly mapped so they can be correctly resolved. This happens through the Address Resolution Protocol (ARP). When the data link layer receives a frame, the network layer has already attached the destination IP address to it, but the data link layer cannot understand the IP address and thus invokes ARP for help. ARP broadcasts a frame requesting the MAC address that corresponds with the destination IP address. Each computer on the subnet receives this broadcast frame, and all but the computer that has the requested IP address ignore it.
The computer that has the destination IP address responds with its MAC address. Now ARP knows what hardware address corresponds with that specific IP address. The data link layer takes the frame, adds the hardware address to it, and passes it on to the physical layer, which enables the frame to hit the wire and go to the destination computer. ARP maps the hardware address and associated IP address and stores this mapping in its table for a predefined amount of time. This caching is done so that when another frame destined for the same IP address needs to hit the wire, ARP does not need to broadcast its request again. It just looks in its table for this information.
Man-In-The-Middle attack
Because ARP does not require authentication, an attacker could place bogus entries into the ARP cache of a remote host (gratuitous ARP replies) to carry out attacks, such as a man-in-the-middle attacks. This attack is called ARP poisoning.
The following answers were incorrect:
RARP is used to match an Ethernet address to an IP address. ICMP is a management protocol whose function is to send message between network devices. Routing tables are used by routers to choose the appropriate interface to route packets.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition, Chapter 6 Telecommunications and Network Security, Pages 580-581 or on the Kindle edition look around Locations 12298-12306. McGraw-Hill. Kindle Edition.
and
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK , Third Edition: Telecommunications and Network Security, Page 342.

QUESTION 331
What protocol is used on the Local Area Network (LAN) to obtain an IP address from it's known MAC address?

A. Reverse address resolution protocol (RARP)
B. Address resolution protocol (ARP)
C. Data link layer
D. Network address translation (NAT)

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The reverse address resolution protocol (RARP) sends out a packet including a MAC address and a request to be informed of the IP address that should be assigned to that MAC.
Diskless workstations do not have a full operating system but have just enough code to know how to boot up and broadcast for an IP address, and they may have a pointer to the server that holds the operating system. The diskless workstation knows its hardware address, so it broadcasts this information so that a listening server can assign it the correct IP address. As with ARP, Reverse Address Resolution Protocol (RARP) frames go to all systems on the subnet, but only the RARP server responds. Once the RARP server receives this request, it looks in its table to see which IP address matches the broadcast hardware address. The server then sends a message that contains its IP address back to the requesting computer. The system now has an IP address and can function on the network.
The Bootstrap Protocol (BOOTP) was created after RARP to enhance the functionality that RARP provides for diskless workstations. The diskless workstation can receive its IP address, the name server address for future name resolutions, and the default gateway address from the BOOTP server. BOOTP usually provides more functionality to diskless workstations than does RARP. The evolution of this protocol has unfolded as follows: RARP evolved into BOOTP, which evolved into DHCP.

The following are incorrect answers:
NAT is a tool that is used for masking true IP addresses by employing internal addresses. ARP does the opposite of RARP, it finds the MAC address that maps with an existing IP address. Data Link layer The Data Link layer is not a protocol; it is represented at layer 2 of the OSI model. In the TCP/IP model, the Data Link and Physical layers are combined into the Network Access layer, which is sometimes called the Link layer or the Network Interface layer.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition, Telecommunications and Network Security, Page 584-585 and also 598. For Kindle users see Kindle Locations 12348- 12357. McGraw-Hill.
and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 87).

QUESTION 332
Which of the following security-focused protocols has confidentiality services operating at a layer different from the others?

A. Secure HTTP (S-HTTP)
B. FTP Secure (FTPS)
C. Secure socket layer (SSL)
D. Sequenced Packet Exchange (SPX)

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: All the previous protocols operate at the transport layer except for Secure HTTP (SHTTP), which operates at the application layer. S-HTTP has been replaced by SSL and TLS.
As it is very well explained in the Shon Harris book:
The transport layer receives data from many different applications and assembles the data into a stream to be properly transmitted over the network. The main protocols that work at this layer are TCP, UDP, Secure Sockets Layer (SSL), and Sequenced Packet Exchange (SPX).
NOTE:
Different references can place specific protocols at different layers. For example, many references place the SSL protocol in the session layer, while other references place it in the transport layer. It is not that one is right or wrong. The OSI model tries to draw boxes around reality, but some protocols straddle the different layers. SSL is made up of two protocols-- one works in the lower portion of the session layer and the other works in the transport layer. For purposes of the CISSP exam, SSL resides in the transport layer.
Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 526). McGraw-Hill.
Kindle Edition.

QUESTION 333
Which type of firewall can be used to track connectionless protocols such as UDP and RPC?

A. Stateful inspection firewalls
B. Packet filtering firewalls
C. Application level firewalls
D. Circuit level firewalls

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Packets in a stateful inspection firewall are queued and then analyzed at all OSI layers, providing a more complete inspection of the data. By examining the state and context of the incoming data packets, it helps to track the protocols that are considered "connectionless", such as UDP-based applications and

Remote Procedure Calls (RPC). Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 91).

QUESTION 334
Which of the following is the most secure firewall implementation?

A. Dual-homed host firewalls
B. Screened-subnet firewalls
C. Screened-host firewalls
D. Packet-filtering firewalls

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: One the most secure implementations of firewall architectures is the screenedsubnet firewall. It employs two packet-filtering routers and a bastion host. Like a screened host firewall, this firewall supports both packet-filtering and proxy services. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 93).

QUESTION 335
Which of the following is NOT a VPN communications protocol standard?

A. Point-to-point tunnelling protocol (PPTP)
B. Challenge Handshake Authentication Protocol (CHAP)
C. Layer 2 tunnelling protocol (L2TP)
D. IP Security

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: CHAP is an authentication mechanism for point-to-point protocol connections that encrypt the user's password. It is a protocol that uses a three-way handshake. The server sends the client a challenge, which includes a random value (a nonce) to thwart replay attacks. The client responds with a MD5 hash of the nonce and the password. The authentication is successful if the client's response is the one that the server expected. The VPN communication protocol standards listed above are PPTP, L2TP and IPSec. PPTP and L2TP operate at the data link layer (layer 2) of the OSI model and enable only a single point-to-point connection per session.
The following are incorrect answers:
PPTP uses native PPP authentication and encryption services. Point-to-Point Tunneling Protocol (PPTP) is a VPN protocol that runs over other protocols. PPTP relies on generic routing encapsulation (GRE) to build the tunnel between the endpoints. After the user authenticates, typically with Microsoft Challenge Handshake Authentication Protocol version 2 (MSCHAPv2), a Point-to-Point Protocol (PPP) session creates a tunnel using GRE. L2TP is a combination of PPTP and the earlier Layer 2 Forwarding protocol (L2F). Layer 2 Tunneling Protocol (L2TP) is a hybrid of Cisco's Layer 2 Forwarding (L2F) and Microsoft's PPTP. It allows callers over a serial line using PPP to connect over the Internet to a remote network. A dial-up user connects to his ISP's L2TP access concentrator (LAC) with a PPP connection. The LAC encapsulates the PPP packets into L2TP and forwards it to the remote network's layer 2 network server (LNS). At this point, the LNS authenticates the dial-up user. If authentication is successful, the dial-up user will have access to the remote network. IPSec operates at the network layer (layer 3) and enables multiple simultaneous tunnels. IP Security (IPSec) is a suite of protocols for communicating securely with IP by providing mechanisms for authenticating and encryption. Implementation of IPSec is mandatory in IPv6, and many organizations are using it over IPv4. Further, IPSec can be implemented in two modes, one that is appropriate for end-to-end protection and one that safeguards traffic between networks.

Reference used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 7067-7071). Auerbach Publications. Kindle Edition.
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 6987-6990). Auerbach Publications. Kindle Edition.

QUESTION 336
What layer of the OSI/ISO model does Point-to-point tunnelling protocol (PPTP) work at?

A. Data link layer
B. Transport layer
C. Session layer
D. Network layer

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: PPTP operates at the data link layer (layer 2) of the OSI model and uses native PPP authentication and encryption services. Designed for individual client to server connections, it enables only a single point-to-point connection per session. PPTP - Point-to-Point Tunneling Protocol - extends the Point to Point Protocol (PPP) standard for traditional dial-up networking. PPTP is best suited for the remote access applications of VPNs, but it also supports LAN internetworking.
PPTP operates at Layer 2 of the OSI model.
Using PPTP
PPTP packages data within PPP packets, then encapsulates the PPP packets within IP packets (datagrams) for transmission through an Internet-based VPN tunnel. PPTP supports data encryption and compression of these packets. PPTP also uses a form of General Routing Encapsulation (GRE) to get data to and from its final destination.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 95).
and
http://compnetworking.about.com/od/vpn/l/aa030103a.htm and
http://technet.microsoft.com/en-us/library/cc768084.aspx

QUESTION 337
Which of the following statements pertaining to VPN protocol standards is false?

A. L2TP is a combination of PPTP and L2F.
B. L2TP and PPTP were designed for single point-to-point client to server communication.
C. L2TP operates at the network layer.
D. PPTP uses native PPP authentication and encryption services.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: L2TP and PPTP were both designed for individual client to server connections; they enable only a single point-to-point connection per session. Dial-up VPNs use L2TP often. Both L2TP and PPTP operate at the data link layer (layer 2) of the OSI model. PPTP uses native PPP authentication and encryption services and L2TP is a combination of PPTP and Layer 2 Forwarding protocol (L2F).
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 95).

QUESTION 338
Which OSI/ISO layer does a SOCKS server operate at?

A. Session layer
B. Transport layer
C. Network layer
D. Data link layer

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: A SOCKS based server operates at the Session layer of the OSI model. SOCKS is an Internet protocol that allows client-server applications to transparently use the services of a network firewall. SOCKS is an abbreviation for "SOCKetS". As of Version 5 of SOCK, both UDP and TCP is supported.
One of the best known circuit-level proxies is SOCKS proxy server. The basic purpose of the protocol is to enable hosts on one side of a SOCKS server to gain access to hosts on the other side of a SOCKS Server, without requiring direct "IP-reachability" The protocol was originally developed by David Koblas, a system administrator of MIPS Computer Systems. After MIPS was taken over by Silicon Graphics in 1992, Koblas presented a paper on SOCKS at that year's Usenix Security Symposium and SOCKS became publicly available. The protocol was extended to version 4 by Ying-Da Lee of NEC. SOCKS includes two components, the SOCKS server and the SOCKS client.
The SOCKS protocol performs four functions:
Making connection requests
Setting up proxy circuits
Relaying application data
Performing user authentication (optional)
Source:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 96).
and
http://en.wikipedia.org/wiki/SOCKS
and
http://www.faqs.org/rfcs/rfc1928.html
and
The ISC2 OIG on page 619

QUESTION 339
Which IPSec operational mode encrypts the entire data packet (including header and data) into an IPSec packet?

A. Authentication mode
B. Tunnel mode
C. Transport mode
D. Safe mode

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: In tunnel mode, the entire packet is encrypted and encased into an IPSec packet. In transport mode, only the datagram (payload) is encrypted, leaving the IP address visible within the IP header. Authentication mode and safe mode are not defined IPSec operational modes. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 96).

QUESTION 340

Which of the following category of UTP cables is specified to be able to handle gigabit Ethernet (1 Gbps) according to the EIA/TIA-568-B standards?

A. Category 5e UTP
B. Category 2 UTP
C. Category 3 UTP
D. Category 1e UTP

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Categories 1 through 6 are based on the EIA/TIA-568-B standards. On the newer wiring for LANs is CAT5e, an improved version of CAT5 which used to be outside of the standard, for more information on twisted pair, please see: twisted pair.
Category Cable Type Mhz Usage Speed
==
CAT1 UTP Analog voice, Plain Old Telephone System (POTS) CAT2 UTP 4 Mbps on Token Ring, also used on Arcnet networks CAT3 UTP, ScTP, STP 16 MHz 10 Mbps
CAT4 UTP, ScTP, STP 20 MHz 16 Mbps on Token Ring Networks CAT5 UTP, ScTP, STP 100 MHz 100 Mbps on ethernet, 155 Mbps on ATM CAT5e UTP, ScTP, STP 100 MHz 1 Gbps (out of standard version, improved version of CAT5) CAT6 UTP, ScTP, STP 250 MHz 10 Gbps
CAT7 ScTP, STP 600 M 100 Gbps
Category 6 has a minumum of 250 MHz of bandwidth. Allowing 10/100/1000 use with up to 100 meter cable length, along with 10GbE over shorter distances. Category 6a or Augmented Category 6 has a minimum of 500 MHz of bandwidth. It is the newest standard and allows up to 10GbE with a length up to 100m. Category 7 is a future cabling standard that should allow for up to 100GbE over 100 meters of cable. Expected availability is in 2013. It has not been approved as a cable standard, and anyone now selling you Cat. 7 cable is fooling you.

http://donutey.com/ethernet.php
http://en.wikipedia.org/wiki/TIA/EIA-568-B
http://en.wikipedia.org/wiki/Category_1_cable

QUESTION 341
Which of the following mechanisms was created to overcome the problem of collisions that occur on wired networks when traffic is simultaneously transmitted from different nodes?

A. Carrier sense multiple access with collision avoidance (CSMA/CA)
B. Carrier sense multiple access with collision detection (CSMA/CD)
C. Polling
D. Token-passing

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 342
Which of the following does NOT use token-passing?

A. ARCnet
B. FDDI
C. Token-ring
D. IEEE 802.3

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: IEEE 802.3 specifies the standard for Ethernet and uses CSMA/CD, not tokenpassing. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 104).

QUESTION 343
What is defined as the manner in which the network devices are organized to facilitate communications?

A. LAN transmission methods
B. LAN topologies
C. LAN transmission protocols
D. LAN media access methods

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: A network topology defines the manner in which the network devices are organized to facilitate communications. Common LAN technologies are:
bus
ring
star
meshed
LAN transmission methods refer to the way packets are sent on the network and are:
unicast
multicast
broadcast
LAN transmission protocols are the rules for communicating between computers on a LAN.
Common LAN transmission protocols are:
CSMA/CD
polling
token-passing
LAN media access methods control the use of a network (physical and data link layers). They can be:
Ethernet
ARCnet
Token ring
FDDI
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 105).

QUESTION 344
Which of the following is a device that is used to regenerate or replicate the received signals?

A. Bridge
B. Router
C. Repeater
D. Brouter

Correct Answer: C
Explanation

Explanation/Reference:

Explanation: Repeaters offer the simplest form of connectivity. They regenerate received electrical signals at their original strength between cable segments. Bridges are devices used to connect similar or dissimilar LANs together to form an extended LAN. Routers provide packet routing between network segments. Brouter are devices that combine router and bridge functionality.

Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 7: Telecommunications and Network Security (page 397).

QUESTION 345

Which of the following networking devices allows the connection of two or more homogeneous LANs in a simple way where they forward the traffic based on the MAC address ?

A. Gateways

B. Routers

C. Bridges

D. Firewalls

Correct Answer: C

Explanation

Explanation/Reference:

Explanation: Bridges are simple, protocol-dependent networking devices that are used to connect two or more homogeneous LANs to form an extended LAN.

A bridge does not change the contents of the frame being transmitted but acts as a relay. A gateway is designed to reduce the problems of interfacing any combination of local networks that employ different level protocols or local and long-haul networks. A router connects two networks or network segments and may use IP to route messages. Firewalls are methods of protecting a network against security threats from other systems or networks by centralizing and controlling access to the protected network segment. Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 7: Telecommunications and Network Security (page 397).

QUESTION 346

Which of the following statements pertaining to Asynchronous Transfer Mode (ATM) is false?

A. It can be used for voice

B. it can be used for data

C. It carries various sizes of packets

D. It can be used for video

Correct Answer: C

Explanation

Explanation/Reference:

Explanation: ATM is an example of a fast packet-switching network that can be used for either data, voice or video, but packets are of fixed size.

Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 7: Telecommunications and Network Security (page 455).

QUESTION 347

Which of the following can prevent hijacking of a web session?

A. RSA

B. SET

C. SSL

D. PPP

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The Secure Socket Layer (SSL) protocol is used between a web server and client and provides entire session encryption, thus preventing from session hijacking. RSA is asymmetric encryption algorithm that can be used in setting up a SSL session. SET is the Secure Electronic Transaction protocol that was introduced by Visa and Mastercard to allow for more credit card transaction possibilities. PPP is a point-to-point protocol. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 89).

QUESTION 348
Which type of attack involves impersonating a user or a system?

A. Smurfing attack
B. Spoofing attack
C. Spamming attack
D. Sniffing attack

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: A spoofing attack is when an attempt is made to gain access to a computer system by posing as an authorized user or system. Spamming refers to sending out or posting junk advertising and unsolicited mail. A smurf attack is a type of denial-of-service attack using PING and a spoofed address. Sniffing refers to observing packets passing on a network. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 77).

QUESTION 349
How would an IP spoofing attack be best classified?

A. Session hijacking attack
B. Passive attack
C. Fragmentation attack
D. Sniffing attack

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: IP spoofing is used to convince a system that it is communicating with a known entity that gives an intruder access. IP spoofing attacks is a common session hijacking attack. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 77).

QUESTION 350
What is defined as the rules for communicating between computers on a Local Area Network (LAN)?

A. LAN Media Access methods
B. LAN topologies
C. LAN transmission methods
D. Contention Access Control

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Media contention occurs when two or more network devices have data to send at the same time. Because multiple devices cannot talk on the network simultaneously, some type of method must be used to allow one device access to the network media at a time. This is done in two main ways: carrier sense multiple access collision detect (CSMA/CD) and token passing.
In networks using CSMA/CD technology such as Ethernet, network devices contend for the network media. When a device has data to send, it first listens to see if any other device is currently using the network. If not, it starts sending its data. After finishing its transmission, it listens again to see if a collision occurred. A collision occurs when two devices send data simultaneously. When a collision happens, each device waits a random length of time before resending its data. In most cases, a collision will not occur again between the two devices. Because of this type of network contention, the busier a network becomes, the more collisions occur. This is why performance of Ethernet degrades rapidly as the number of devices on a single network increases.
In token-passing networks such as Token Ring and FDDI, a special network frame called a token is passed around the network from device to device. When a device has data to send, it must wait until it has the token and then sends its data. When the data transmission is complete, the token is released so that other devices may use the network media. The main advantage of token-passing networks is that they are deterministic. In other words, it is easy to calculate the maximum time that will pass before a device has the opportunity to send data. This explains the popularity of token-passing networks in some real-time environments such as factories, where machinery must be capable of communicating at a determinable interval. For CSMA/CD networks, switches segment the network into multiple collision domains. This reduces the number of devices per network segment that must contend for the media. By creating smaller collision domains, the performance of a network can be increased significantly without requiring addressing changes.
The following are incorrect answers:
LAN topologies: Think of a topology as a network's virtual shape or structure. This shape does not necessarily correspond to the actual physical layout of the devices on the network. For example, the computers on a home LAN may be arranged in a circle in a family room, but it would be highly unlikely to find a ring topology there. Common topologies are: bus, ring, star or meshed. See THIS LINK for more information.
LAN transmission methods: refer to the way packets are sent on the network and are either unicast, multicast or broadcast. See THIS LINK for more information.
Contention Access Control: This is a bogus detractor.
Contention is a real term but Contention Access Control is just made up. Contention methods is very closely related to Media Access Control methods. In communication networks, contention is a media access method that is used to share a broadcast medium. In contention, any computer in the network can transmit data at any time (first come-first served). This system breaks down when two computers attempt to transmit at the same time. This is a case of collision. To avoid collision, carrier sensing mechanism is used. Here each computer listens to the network before attempting to transmit. If the network is busy, it waits until network quiets down. In carrier detection, computers continue to listen to the network as they transmit. If computer detects another signal that interferes with the signal it is sending, it stops transmitting. Both computers then wait for random amount of time and attempt to transmit. Contention methods are most popular media access control method on LANs.
Reference(s) used for this question:
http://docwiki.cisco.com/wiki/Introduction_to_LAN_Protocols#LAN_Media-Access_Methods http://en.wikipedia.org/wiki/Contention_%28telecommunications%29

QUESTION 351
Which of the following is a LAN transmission method?

A. Broadcast
B. Carrier-sense multiple access with collision detection (CSMA/CD)
C. Token ring
D. Fiber Distributed Data Interface (FDDI)

Correct Answer: A
Explanation

Explanation/Reference:

Explanation: LAN transmission methods refer to the way packets are sent on the network and are either unicast, multicast or broadcast.

CSMA/CD is a common LAN media access method.

Token ring is a LAN Topology.

LAN transmission protocols are the rules for communicating between computers on a LAN. Common LAN transmission protocols are: polling and token-passing. A LAN topology defines the manner in which the network devices are organized to facilitate communications.

Common LAN topologies are: bus, ring, star or meshed.

LAN transmission methods refer to the way packets are sent on the network and are either unicast, multicast or broadcast.

LAN media access methods control the use of a network (physical and data link layers). They can be Ethernet, ARCnet, Token ring and FDDI.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 103).

HERE IS A NICE OVERVIEW FROM CISCO:

LAN Transmission Methods

LAN data transmissions fall into three classifications: unicast, multicast, and broadcast. In each type of transmission, a single packet is sent to one or more nodes. In a unicast transmission, a single packet is sent from the source to a destination on a network. First, the source node addresses the packet by using the address of the destination node. The package is then sent onto the network, and finally, the network passes the packet to its destination.

A multicast transmission consists of a single data packet that is copied and sent to a specific subset of nodes on the network. First, the source node addresses the packet by using a multicast address. The packet is then sent into the network, which makes copies of the packet and sends a copy to each node that is part of the multicast address. A broadcast transmission consists of a single data packet that is copied and sent to all nodes on the network. In these types of transmissions, the source node addresses the packet by using the broadcast address. The packet is then sent on to the network, which makes copies of the packet and sends a copy to every node on the network.

LAN Topologies

LAN topologies define the manner in which network devices are organized. Four common LAN topologies exist: bus, ring, star, and tree. These topologies are logical architectures, but the actual devices need not be physically organized in these configurations. Logical bus and ring topologies, for example, are commonly organized physically as a star. A bus topology is a linear LAN architecture in which transmissions from network stations propagate the length of the medium and are received by all other stations. Of the three most widely used LAN implementations, Ethernet/IEEE 802.3 networks--including 100BaseT--implement a bus topology

Sources:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 104).

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introlan.htm

QUESTION 352

Which of the following LAN topologies offers the highest availability?

A. Bus topology

B. Tree topology

C. Full mesh topology

D. Partial mesh topology

Correct Answer: C

Explanation

Explanation/Reference:

Explanation: In a full mesh topology, all network nodes are individually connected with each other, providing the highest availability. A partial mesh topology can sometimes be used to offer some redundancy.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of

Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 106).

QUESTION 353
What is also known as 10Base5?

A. Thinnet
B. Thicknet
C. ARCnet
D. UTP

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Thicknet is a coaxial cable with segments of up to 500 meters, also known as 10Base5. Thinnet is a coaxial cable with segments of up to 185 meters. Unshielded twisted pair (UTP) has three variations: 10 Mbps (10BaseT), 100 Mbps (100BaseT) or 1 Gbps (1000BaseT).
ARCnet is a LAN media access method.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 108).

QUESTION 354
Which of the following is an example of a connectionless communication protocol?

A. UDP
B. X.25
C. Packet switching
D. TCP

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: UDP is an example of connectionless communication protocol, wherein no connection needs to be established before data can be exchanged. In telecommunications, connectionless describes communication between two network end points in which a message can be sent from one end point to another without prior arrangement. The device at one end of the communication transmits data addressed to the other, without first ensuring that the recipient is available and ready to receive the data. Some protocols allow for error correction by requested retransmission. Internet Protocol (IP) and User Datagram Protocol (UDP) are connectionless protocols.
Connectionless protocols are also described as stateless because the endpoints have no protocoldefined way to remember where they are in a "conversation" of message exchanges.
List of connectionless protocols
Hypertext Transfer Protocol
IP
UDP
ICMP
IPX
TIPC
NetBEUI

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 86).
and
https://secure.wikimedia.org/wikipedia/en/wiki/Connectionless_protocol

QUESTION 355
Which of the following standards is concerned with message handling?

A. X.400
B. X.500
C. X.509
D. X.800

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: X.400 is used in e-mail as a message handling protocol. X.500 is used in directory services. X.509 is used in digital certificates and X.800 is used a network security standard.
http://www.alvestrand.no/x400/.

QUESTION 356
Which of the following IEEE standards defines the token ring media access method?

A. 802.3
B. 802.11
C. 802.5
D. 802.2

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The IEEE 802.5 standard defines the token ring media access method. 802.3 refers to Ethernet's CSMA/CD, 802.11 refers to wireless communications and 802.2 refers to the logical link control.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 109).

QUESTION 357
Which of the following technologies has been developed to support TCP/IP networking over lowspeed serial interfaces?

A. ISDN
B. SLIP
C. xDSL
D. T1

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Serial Line IP (SLIP) was developed in 1984 to support TCP/IP networking over lowspeed serial interfaces.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 114).

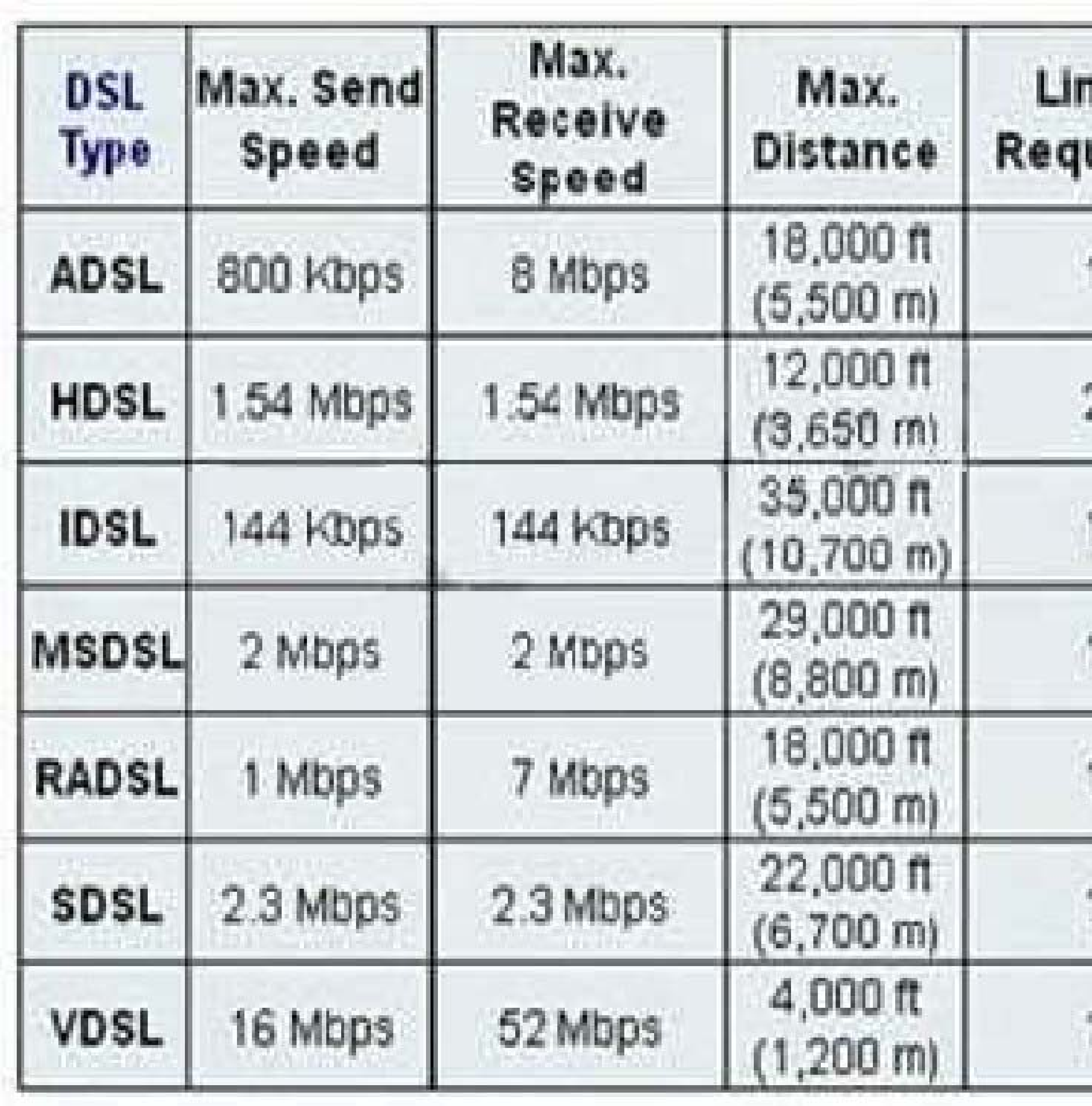
QUESTION 358
Which xDSL flavour, appropriate for home or small offices, delivers more bandwidth downstream than

upstream and over longer distance?

A. VDSL
B. SDSL
C. ADSL
D. HDSL

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Asymmetric digital subscriber line (ADSL) is designed to provide more bandwidth downstream (1 to 8 Mbps) than upstream (16 to 800Kb).
DSL (Digital Subscriber Line) is a modem technology for broadband data access over ordinary copper telephone lines (POTS) from homes and businesses. xDSL refers collectively to all types of DSL, such as ADSL (and G.Lite), HDSL, SDSL, IDSL and VDSL etc. They are sometimes referred to as last-mile (or first mile) technologies because they are used only for connections from a telephone switching station to a home or office, not between switching stations. xDSL is similar to ISDN in as much as both operate over existing copper telephone lines (POTS) using sophisticated modulation schemes and both require the short runs to a central telephone office
Graphic below from: http://computer.howstuffworks.com/vdsl3.htm



DSL Type	Max. Send Speed	Max. Receive Speed	Max. Distance	Lin Requ
ADSL	800 Kbps	8 Mbps	18,000 ft (5,500 m)	1
HDSL	1.54 Mbps	1.54 Mbps	12,000 ft (3,650 m)	2
IDSL	144 Kbps	144 Kbps	35,000 ft (10,700 m)	1
MSDSL	2 Mbps	2 Mbps	29,000 ft (8,800 m)	1
RADSL	1 Mbps	7 Mbps	18,000 ft (5,500 m)	1
SDSL	2.3 Mbps	2.3 Mbps	22,000 ft (6,700 m)	1
VDSL	16 Mbps	52 Mbps	4,000 ft (1,200 m)	1

DSL speed chart
The following are incorrect answers:
Single-line Digital Subscriber Line (SDSL) deliver 2.3 Mbps of bandwidth each way. High-rate Digital Subscriber Line (HDSL) deliver 1.544 Mbps of bandwidth each way. Very-high data-rate Digital Subscriber Line (VDSL) can deliver up to 52 Mbps downstream over a single copper twisted pair over a relatively short distance (1000 to 4500 feet).
Reference used for this question:
http://computer.howstuffworks.com/vdsl3.htm

and
http://www.javvin.com/protocolxDSL.html
and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 115).

QUESTION 359
What ISO/OSI layer do switches primarily operate at?
Do take note that this question makes reference to a plain vanilla switch and not one of the smart switches that is available on the market today.

A. Physical layer
B. Network layer
C. Data link layer
D. Session layer

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Switches primarily operate at the data link layer (layer 2), although intelligent, extremely fast Layer 3 switching techniques are being more frequently used. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 111).

QUESTION 360
Which xDSL flavour delivers both downstream and upstream speeds of 1.544 Mbps over two copper twisted pairs?

A. HDSL
B. SDSL
C. ADSL
D. VDSL

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: High-rate Digital Subscriber Line (HDSL) delivers 1.544 Mbps of bandwidth each way over two copper twisted pairs. SDSL also delivers 1.544 Mbps but over a single copper twisted pair. ADSL and VDSL offer a higher bandwidth downstream than upstream. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 115).

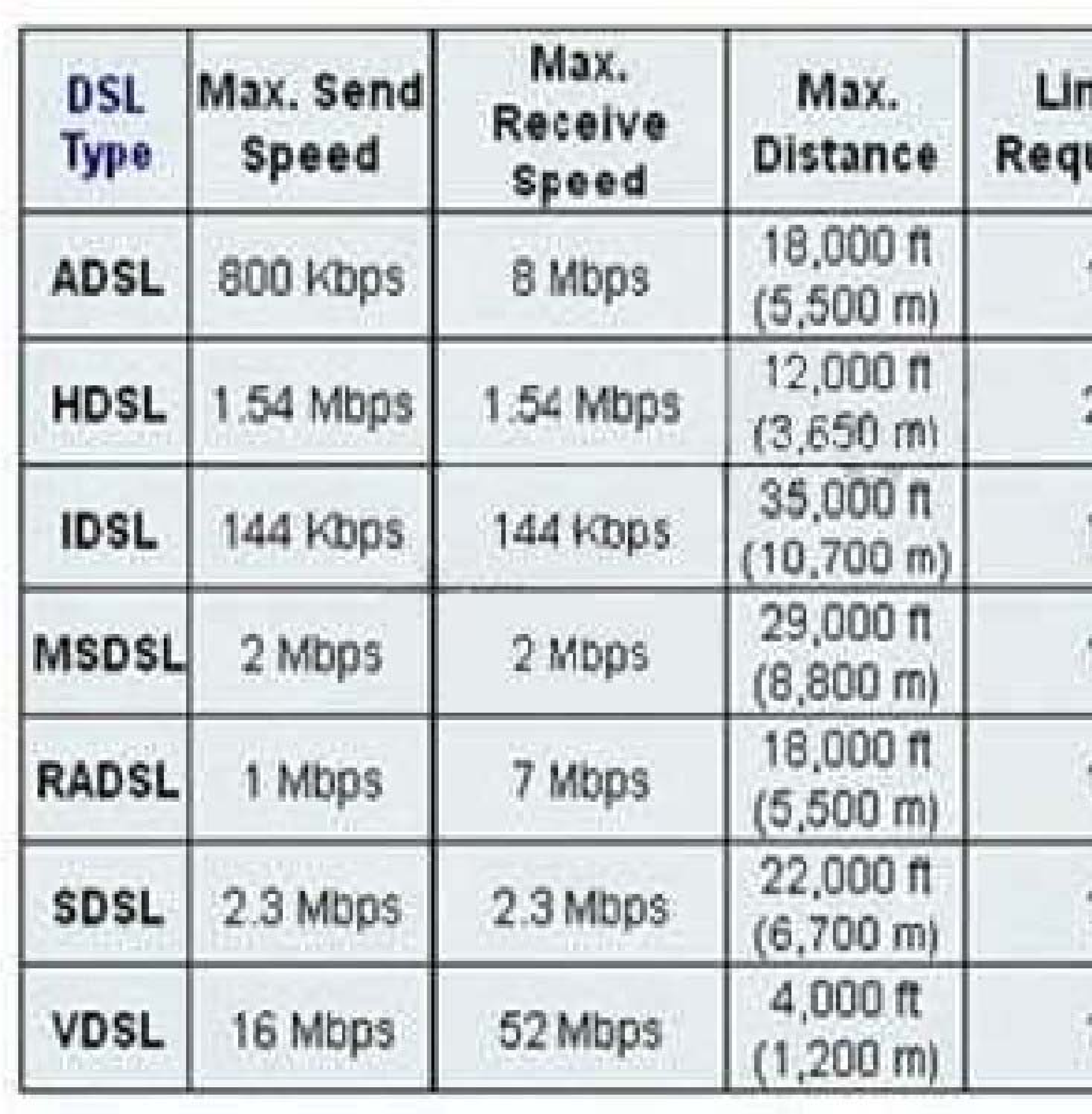
QUESTION 361
Which xDSL flavour can deliver up to 52 Mbps downstream over a single copper twisted pair?

A. VDSL
B. SDSL
C. HDSL
D. ADSL

Correct Answer: A
Explanation

Explanation/Reference:

Explanation: Very-high data-rate Digital Subscriber Line (VDSL) can deliver up to 52 Mbps downstream over a single copper twisted pair over a relatively short distance (1000 to 4500 feet). DSL (Digital Subscriber Line) is a modem technology for broadband data access over ordinary copper telephone lines (POTS) from homes and businesses. xDSL refers collectively to all types of DSL, such as ADSL (and G.Lite), HDSL, SDSL, IDSL and VDSL etc. They are sometimes referred to as last-mile (or first mile) technologies because they are used only for connections from a telephone switching station to a home or office, not between switching stations. xDSL is similar to ISDN in as much as both operate over existing copper telephone lines (POTS) using sophisticated modulation schemes and both require the short runs to a central telephone office
Graphic below from: http://computer.howstuffworks.com/vdsl3.htm



DSL Type	Max. Send Speed	Max. Receive Speed	Max. Distance	Lin Requ
ADSL	800 Kbps	8 Mbps	18,000 ft (5,500 m)	1
HDSL	1.54 Mbps	1.54 Mbps	12,000 ft (3,650 m)	2
IDSL	144 Kbps	144 Kbps	35,000 ft (10,700 m)	1
MSDSL	2 Mbps	2 Mbps	29,000 ft (8,800 m)	1
RADSL	1 Mbps	7 Mbps	18,000 ft (5,500 m)	1
SDSL	2.3 Mbps	2.3 Mbps	22,000 ft (6,700 m)	1
VDSL	16 Mbps	52 Mbps	4,000 ft (1,200 m)	1

DSL speed chart
The following are incorrect answers:
Single-line Digital Subscriber Line (SDSL) deliver 2.3 Mbps of bandwidth each way. High-rate Digital Subscriber Line (HDSL) deliver 1.544 Mbps of bandwidth each way. ADSL delivers a maximum of 8 Mbps downstream for a total combined speed of almost 9 Mbps up and down.
Reference used for this question:
http://computer.howstuffworks.com/vdsl3.htm
and

http://www.javvin.com/protocolxDSL.html
and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 115).

QUESTION 362
What is the framing specification used for transmitting digital signals at 1.544 Mbps on a T1 facility?

A. DS-0
B. DS-1
C. DS-2
D. DS-3

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Digital Signal level 1 (DS-1) is the framing specification used for transmitting digital signals at 1.544 Mbps on a T1 facility. DS-0 is the framing specification used in transmitting digital signals over a single 64 Kbps channel over a T1 facility. DS-3 is the framing specification used for transmitting digital signals at 44.736 Mbps on a T3 facility. DS-2 is not a defined framing specification.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 114).

QUESTION 363
Which of the following is the biggest concern with firewall security?

A. Internal hackers
B. Complex configuration rules leading to misconfiguration
C. Buffer overflows
D. Distributed denial of service (DDOS) attacks

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Firewalls tend to give a false sense of security. They can be very hard to bypass but they need to be properly configured. The complexity of configuration rules can introduce a vulnerability when the person responsible for its configuration does not fully understand all possible options and switches. Denial of service attacks mainly concerns availability. Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 3: Telecommunications and Network Security (page 412).

QUESTION 364
Which of the following is the simplest type of firewall ?

A. Stateful packet filtering firewall
B. Packet filtering firewall
C. Dual-homed host firewall
D. Application gateway

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: A static packet filtering firewall is the simplest and least expensive type of firewalls, offering

minimum security provisions to a low-risk computing environment. A static packet filter firewall examines both the source and destination addresses of the incoming data packet and applies ACL's to them. They operates at either the Network or Transport layer.

They are known as the First generation of firewall.

Older firewalls that were only packet filters were essentially routing devices that provided access control functionality for host addresses and communication sessions. These devices, also known as stateless inspection firewalls, do not keep track of the state of each flow of traffic that passes though the firewall; this means, for example, that they cannot associate multiple requests within a single session to each other. Packet filtering is at the core of most modern firewalls, but there are few firewalls sold today that only do stateless packet filtering. Unlike more advanced filters, packet filters are not concerned about the content of packets. Their access control functionality is governed by a set of directives referred to as a ruleset. Packet filtering capabilities are built into most operating systems and devices capable of routing; the most common example of a pure packet filtering device is a network router that employs access control lists.

There are many types of Firewall:

Application Level Firewalls Often called a Proxy Server. It works by transferring a copy of each accepted data packet from one network to another. They are known as the Second generation of firewalls.

An application-proxy gateway is a feature of advanced firewalls that combines lower-layer access control with upper-layer functionality. These firewalls contain a proxy agent that acts as an intermediary between two hosts that wish to communicate with each other, and never allows a direct connection between them. Each successful connection attempt actually results in the creation of two separate connections--one between the client and the proxy server, and another between the proxy server and the true destination. The proxy is meant to be transparent to the two hosts--from their perspectives there is a direct connection. Because external hosts only communicate with the proxy agent, internal IP addresses are not visible to the outside world. The proxy agent interfaces directly with the firewall ruleset to determine whether a given instance of network traffic should be allowed to transit the firewall. Stateful Inspection Firewall - Packets are captured by the inspection engine operating at the network layer and then analyzed at all layers. They are known as the Third generation of firewalls. Stateful inspection improves on the functions of packet filters by tracking the state of connections and blocking packets that deviate from the expected state. This is accomplished by incorporating greater awareness of the transport layer. As with packet filtering, stateful inspection intercepts packets at the network layer and inspects them to see if they are permitted by an existing firewall rule, but unlike packet filtering, stateful inspection keeps track of each connection in a state table. While the details of state table entries vary by firewall product, they typically include source IP address, destination IP address, port numbers, and connection state information. Web Application Firewalls - The HTTP protocol used in web servers has been exploited by attackers in many ways, such as to place malicious software on the computer of someone browsing the web, or to fool a person into revealing private information that they might not have otherwise. Many of these exploits can be detected by specialized application firewalls called web application firewalls that reside in front of the web server. Web application firewalls are a relatively new technology, as compared to other firewall technologies, and the type of threats that they mitigate are still changing frequently. Because they are put in front of web servers to prevent attacks on the server, they are often considered to be very different than traditional firewalls.

Host-Based Firewalls and Personal Firewalls - Host-based firewalls for servers and personal firewalls for desktop and laptop personal computers (PC) provide an additional layer of security against network-based attacks. These firewalls are software-based, residing on the hosts they are protecting--each monitors and controls the incoming and outgoing network traffic for a single host. They can provide more granular protection than network firewalls to meet the needs of specific hosts.

Host-based firewalls are available as part of server operating systems such as Linux, Windows, Solaris, BSD, and Mac OS X Server, and they can also be installed as third-party add-ons. Configuring a host-based firewall to allow only necessary traffic to the server provides protection against malicious activity from all hosts, including those on the same subnet or on other internal subnets not separated by a network firewall. Limiting outgoing traffic from a server may also be helpful in preventing certain malware that infects a host from spreading to other hosts.11 Hostbased firewalls usually perform logging, and can often be configured to perform address-based and application-based access controls

Dynamic Packet Filtering Makes informed decisions on the ACL's to apply. They are known as the Fourth generation of firewalls.

Kernel Proxy - Very specialized architecture that provides modular kernel-based, multi-layer evaluation and runs in the NT executive space. They are known as the Fifth generation of firewalls.

The following were incorrect answers:

All of the other types of firewalls listed are more complex than the Packet Filtering Firewall.

Reference(s) used for this question:

HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 6th Edition, Telecommunications and Network Security, Page 630.
and
NIST Guidelines on Firewalls and Firewalls policies, Special Publication 800-4 Revision 1

QUESTION 365
Upon which of the following ISO/OSI layers does network address translation operate?

A. Transport layer
B. Session layer
C. Data link layer
D. Network layer

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Network address translation (NAT) is concerned with IP address translation between two networks and operates at the network layer (layer 3). Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 3: Telecommunications and Network Security (page 440).

QUESTION 366
Which of the following devices enables more than one signal to be sent out simultaneously over one physical circuit?

A. Router
B. Multiplexer
C. Channel service unit/Data service unit (CSU/DSU)
D. Wan switch

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Multiplexers are devices that enable enables more than one signal to be sent out simultaneously over one physical circuit.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 118).

QUESTION 367
What layer of the ISO/OSI model do routers normally operate at?

A. Data link layer
B. Session layer
C. Transport layer
D. Network layer

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Routers are switching devices that operate at the network layer (layer 3) by examining network addresses.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page

111).

QUESTION 368
Which of the following is NOT an advantage that TACACS+ has over TACACS?

A. Event logging
B. Use of two-factor password authentication
C. User has the ability to change his password
D. Ability for security tokens to be resynchronized

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Although TACACS+ provides better audit trails, event logging is a service that is provided with TACACS.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 121).

QUESTION 369
Which of the following remote access authentication systems is the most robust?

A. TACACS+
B. RADIUS
C. PAP
D. TACACS

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: TACACS+ is a proprietary Cisco enhancement to TACACS and is more robust than RADIUS. PAP is not a remote access authentication system but a remote node security protocol. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 122).

QUESTION 370
Which of the following is true about link encryption?

A. Each entity has a common key with the destination node.
B. Encrypted messages are only decrypted by the final node.
C. This mode does not provide protection if anyone of the nodes along the transmission path is compromised.
D. Only secure nodes are used in this type of transmission.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: In link encryption, each entity has keys in common with its two neighboring nodes in the transmission chain.
Thus, a node receives the encrypted message from its predecessor, decrypts it, and then reencrypts it with a new key, common to the successor node. Obviously, this mode does not provide protection if anyone of the nodes along the transmission path is compromised. Encryption can be performed at different communication levels, each with different types of protection and implications. Two general modes of encryption implementation are link encryption and end-to-end encryption.

Link encryption encrypts all the data along a specific communication path, as in a satellite link, T3 line, or telephone circuit. Not only is the user information encrypted, but the header, trailers, addresses, and routing data that are part of the packets are also encrypted. The only traffic not encrypted in this technology is the data link control messaging information, which includes instructions and parameters that the different link devices use to synchronize communication methods. Link encryption provides protection against packet sniffers and eavesdroppers. In end-to-end encryption, the headers, addresses, routing, and trailer information are not encrypted, enabling attackers to learn more about a captured packet and where it is headed.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (pp. 845-846). McGraw-Hill.
And:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 132).

QUESTION 371
Which of the following protects Kerberos against replay attacks?

A. Tokens
B. Passwords
C. Cryptography
D. Time stamps

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: A replay attack refers to the recording and retransmission of packets on the network. Kerberos uses time stamps, which protect against this type of attack. Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 8: Cryptography (page 581).

QUESTION 372
Which of the following offers security to wireless communications?

A. S-WAP
B. WTLS
C. WSP
D. WDP

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Wireless Transport Layer Security (WTLS) is a communication protocol that allows wireless devices to send and receive encrypted information over the Internet. S-WAP is not defined. WSP (Wireless Session Protocol) and WDP (Wireless Datagram Protocol) are part of Wireless Access Protocol (WAP).
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 173).

QUESTION 373
A Wide Area Network (WAN) is basically everything outside of:

A. a Local Area Network (LAN).
B. a Campus Area Network (CAN).
C. a Metropolitan Area Network (MAN).
D. the Internet.

Correct Answer: A

Explanation

Explanation/Reference:
Explanation: A WAN is basically everything outside of a LAN. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 99.

QUESTION 374
Asynchronous Communication transfers data by sending:

A. bits of data sequentially
B. bits of data sequentially in irregular timing patterns
C. bits of data in sync with a heartbeat or clock
D. bits of data simultaneously

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Asynchronous Communication transfers data by sending bits of data in irregular timing patterns. In asynchronous transmission each character is transmitted separately, that is one character at a time. The character is preceded by a start bit, which tells the receiving end where the character coding begins, and is followed by a stop bit, which tells the receiver where the character coding ends. There will be intervals of ideal time on the channel shown as gaps. Thus there can be gaps between two adjacent characters in the asynchronous communication scheme. In this scheme, the bits within the character frame (including start, parity and stop bits) are sent at the baud rate. The START BIT and STOP BIT including gaps allow the receiving and sending computers to synchronise the data transmission. Asynchronous communication is used when slow speed peripherals communicate with the computer. The main disadvantage of asynchronous communication is slow speed transmission. Asynchronous communication however, does not require the complex and costly hardware equipments as is required for synchronous transmission. Asynchronous communication is transmission of data without the use of an external clock signal. Any timing required to recover data from the communication symbols is encoded within the symbols. The most significant aspect of asynchronous communications is variable bit rate, or that the transmitter and receiver clock generators do not have to be exactly synchronized. The asynchronous communication technique is a physical layer transmission technique which is most widely used for personal computers providing connectivity to printers, modems, fax machines, etc.
An asynchronous link communicates data as a series of characters of fixed size and format. Each character is preceded by a start bit and followed by 1-2 stop bits. Parity is often added to provide some limited protection against errors occurring on the link. The use of independent transmit and receive clocks constrains transmission to relatively short characters (<8 bits) and moderate data rates (< 64 kbps, but typically lower).
The asynchronous transmitter delimits each character by a start sequence and a stop sequence. The start bit (0), data (usually 8 bits plus parity) and stop bit(s) (1) are transmitted using a shift register clocked at the nominal data rate.
When asynchronous transmission is used to support packet data links (e.g. IP), then special characters have to be used ("framing") to indicate the start and end of each frame transmitted. One character (none as an escape character) is reserved to mark any occurrence of the special characters within the frame. In this way the receiver is able to identify which characters are part of the frame and which are part of the "framing". Packet communication over asynchronous links is used by some users to get access to a network using a modem.
Most Wide Area Networks use synchronous links and a more sophisticated link protocol Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 100.
and
http://en.wikipedia.org/wiki/Asynchronous_communication and
http://www.erg.abdn.ac.uk/users/gorry/course/phy-pages/async.html and
http://www.ligaturesoft.com/data_communications/async-data-transmission.html

QUESTION 375

Communications devices must operate:

A. at different speeds to communicate.
B. at the same speed to communicate.
C. at varying speeds to interact.
D. at high speed to interact.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Communications devices must operate at the same speed to communicate. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 100.

QUESTION 376
The basic language of modems and dial-up remote access systems is:

A. Asynchronous Communication.
B. Synchronous Communication.
C. Asynchronous Interaction.
D. Synchronous Interaction.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Asynchronous Communication is the basic language of modems and dial-up remote access systems.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 100.

QUESTION 377
Which communication method is characterized by very high speed transmission rates that are governed by electronic clock timing signals?

A. Asynchronous Communication.
B. Synchronous Communication.
C. Automatic Communication.
D. Full duplex Communication.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Synchronous Communication is characterized by very high speed transmission rates that are governed by electronic clock timing signals. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 100

QUESTION 378
Domain Name Service is a distributed database system that is used to map:

A. Domain Name to IP addresses.
B. MAC addresses to domain names.
C. MAC Address to IP addresses.

D. IP addresses to MAC Addresses.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The Domain Name Service is a distributed database system that is used to map domain names to IP addresses and IP addresses to domain names. The Domain Name System is maintained by a distributed database system, which uses the clientserver model. The nodes of this database are the name servers. Each domain has at least one authoritative DNS server that publishes information about that domain and the name servers of any domains subordinate to it. The top of the hierarchy is served by the root nameservers, the servers to query when looking up (resolving) a TLD.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 100.
and
https://en.wikipedia.org/wiki/Domain_Name_System

QUESTION 379
The communications products and services, which ensure that the various components of a network (such as devices, protocols, and access methods) work together refers to:

A. Netware Architecture.
B. Network Architecture.
C. WAN Architecture.
D. Multiprotocol Architecture.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: A Network Architecture refers to the communications products and services, which ensure that the various components of a network (such as devices, protocols, and access methods) work together.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 101.

QUESTION 380
Network cabling comes in three flavors, they are:

A. twisted pair, coaxial, and fiber optic.
B. tagged pair, coaxial, and fiber optic.
C. trusted pair, coaxial, and fiber optic.
D. twisted pair, control, and fiber optic.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Network cabling comes in three flavors: twisted pair, coaxial, and fiber optic.
Twisted pair
Twisted pair cabling is a form of wiring in which two wires (the forward and return conductors of a single circuit) are twisted together for the purposes of canceling out electromagnetic interference (EMI) from external sources. This type of cable is used for home and corporate Ethernet networks. Twisted pair cables consist of two insulated copper wires. There are three types of twisted pair cables: Shielded, Unshielded and Foil
Fiber Optic cable
An optical fiber cable consists of a center glass core surrounded by several layers of protective material. The outer insulating jacket is made of Teflon or PVC to prevent interference. It is expensive but has higher

bandwidth and can transmit data over longer distances.
Coaxial cable
Coaxial lines confine the electromagnetic wave to area inside the cable, between the center conductor and the shield. The transmission of energy in the line occurs totally through the dielectric inside the cable between the conductors. Coaxial lines can therefore be bent and twisted (subject to limits) without negative effects, and they can be strapped to conductive supports without inducing unwanted currents in them and though. The most common use for coaxial cables is for television and other signals with bandwidth of multiple megahertz. Although in most homes coaxial cables have been installed for transmission of TV signals, new technologies (such as the ITU-T G.hn standard) open the possibility of using home coaxial cable for high-speed home networking applications (Ethernet over coax). See the following page for more details: http://fcit.usf.edu/network/chap4/chap4.htm Reference used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 101.
and
Wikipedia at http://en.wikipedia.org/wiki/Networking_cables

QUESTION 381
Unshielded Twisted Pair cabling is a:

A. four-pair wire medium that is used in a variety of networks.
B. three-pair wire medium that is used in a variety of networks.
C. two-pair wire medium that is used in a variety of networks.
D. one-pair wire medium that is used in a variety of networks.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Unshielded Twisted Pair cabling is a four-pair wire medium that is used in a variety of networks.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 101.

QUESTION 382
Unshielded Twisted Pair (UTP) cables comes in several categories. The categories are based on:

A. The level of performance
B. How thick the shielding is.
C. The length of the cable
D. The diameter of the copper.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: TIA/EIA-568 is a set of telecommunications standards from the Telecommunications Industry Association, an offshoot of the EI
A. The standards address commercial building cabling
for telecom products and services.
The standard is currently (2009) at revision C, replacing the 2001 revision B, the 1995 revision A, and the initial issue of 1991, which are now obsolete. Perhaps the best known features of TIA/EIA-568 are the pin/pair assignments for eight-conductor 100-ohm balanced twisted pair cabling. These assignments are named T568A and T568B, and are frequently referred to (erroneously) as TIA/EIA-568A and TIA/EIA-568B. An IEC standard ISO/IEC 11801 provides similar standards for network cables. The standard defines categories of unshielded twisted pair cable systems, with different levels of performance in signal bandwidth, attenuation, and cross-talk. Generally increasing category numbers correspond with a cable system suitable for higher rates of data transmission. Category 3 cable was suitable for telephone circuits and data rates up to 16 million bits per second. Category 5 cable, with more restrictions on attenuation and cross talk, has a bandwidth of 100

MHz. The 1995 edition of the standard defined categories 3, 4, and 5. Categories 1 and 2 were excluded from the standard since these categories were only used for voice circuits, not for data. Twisted pair cabling is a type of wiring in which two conductors of a single circuit are twisted together for the purposes of canceling out electromagnetic interference (EMI) from external sources; for instance, electromagnetic radiation from unshielded twisted pair (UTP) cables, and crosstalk between neighboring pairs. It was invented by Alexander Graham Bell.
SOME OF THE LIMITATION OF UTP
UTP has several drawbacks. Because it does not have shielding like shielded twisted-pair cables, UTP is susceptible to interference from external electrical sources, which could reduce the integrity of the signal. Also, to intercept transmitted data, an intruder can install a tap on the cable or monitor the radiation from the wire. Thus, UTP may not be a good choice when transmitting very sensitive data or when installed in an environment with much electromagnetic interference (EMI) or radio frequency interference (RFI). Despite its drawbacks, UTP is the most common cable type. UTP is inexpensive, can be easily bent during installation, and, in most cases, the risk from the above drawbacks is not enough to justify more expensive cables.
Resource(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 6507-6511). Auerbach Publications. Kindle Edition.
http://en.wikipedia.org/wiki/TIA/EIA-568#cite_note-7
http://en.wikipedia.org/wiki/Twisted_pair
AIOv3 Telecommunication and Networking Security (page 455)

QUESTION 383
In the UTP category rating, the tighter the wind:

A. the higher the rating and its resistance against interference and crosstalk.
B. the slower the rating and its resistance against interference and attenuation.
C. the shorter the rating and its resistance against interference and attenuation.
D. the longer the rating and its resistance against interference and attenuation.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The category rating is based on how tightly the copper cable is wound within the shielding: The tighter the wind, the higher the rating and its resistance against interference and crosstalk.
Twisted pair copper cabling is a form of wiring in which two conductors are wound together for the purposes of canceling out electromagnetic interference (EMI) from external sources and crosstalk from neighboring wires. Twisting wires decreases interference because the loop area between the wires (which determines the magnetic coupling into the signal) is reduced. In balanced pair operation, the two wires typically carry equal and opposite signals (differential mode) which are combined by subtraction at the destination. The noise from the two wires cancel each other in this subtraction because the two wires have been exposed to similar EMI. The twist rate (usually defined in twists per metre) makes up part of the specification for a given type of cable. The greater the number of twists, the greater the attenuation of crosstalk. Where pairs are not twisted, as in most residential interior telephone wiring, one member of the pair may be closer to the source than the other, and thus exposed to slightly different induced EMF. KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 101.
and
http://www.consultants-online.co.za/pub/itap_101/html/ch04s05.html

QUESTION 384
In this type of attack, the intruder re-routes data traffic from a network device to a personal machine. This diversion allows an attacker to gain access to critical resources and user credentials, such as passwords, and to gain unauthorized access to critical systems of an organization. Pick the best choice below.

A. Network Address Translation
B. Network Address Hijacking
C. Network Address Supernetting

D. Network Address Sniffing

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Network address hijacking allows an attacker to reroute data traffic from a network device to a personal computer.
Also referred to as session hijacking, network address hijacking enables an attacker to capture and analyze the data addressed to a target system. This allows an attacker to gain access to critical resources and user credentials, such as passwords, and to gain unauthorized access to critical systems of an organization.
Session hijacking involves assuming control of an existing connection after the user has successfully created an authenticated session. Session hijacking is the act of unauthorized insertion of packets into a data stream.
It is normally based on sequence number attacks, where sequence numbers are either guessed or intercepted.
The following are incorrect answers:
Network address translation (NAT) is a methodology of modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device for the purpose of remapping one IP address space into another. See RFC 1918 for more details.
Network Address Supernetting There is no such thing as Network Address Supernetting. However, a supernetwork, or supernet, is an Internet Protocol (IP) network that is formed from the combination of two or more networks (or subnets) with a common Classless Inter-Domain Routing (CIDR) prefix. The new routing prefix for the combined network aggregates the prefixes of the constituent networks.
Network Address Sniffing This is another bogus choice that sound good but does not even exist. However, sniffing is a common attack to capture cleartext password and information unencrypted over the network.
Sniffier is accomplished using a sniffer also called a Protocol Analyzer. A network sniffers monitors data flowing over computer network links. It can be a self-contained software program or a hardware device with the appropriate software or firmware programming. Also sometimes called "network probes" or "snoops," sniffers examine network traffic, making a copy of the data but without redirecting or altering it. The following reference (s) were used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 8641-8642). Auerbach Publications. Kindle Edition. http://compnetworking.about.com/od/networksecurityprivacy/g/bldef_sniffer.htm http://wiki.answers.com/Q/What_is_network_address_hijacking KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 239.

QUESTION 385
What works as an E-mail message transfer agent?

A. SMTP
B. SNMP
C. S-RPC
D. S/MIME

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: SMTP (Simple Mail Transfer Protocol) works as a message transfer agent. Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, Page 821.

QUESTION 386
What is the main characteristic of a multi-homed host?

A. It is placed between two routers or firewalls.
B. It allows IP routing.
C. It has multiple network interfaces, each connected to separate networks.

D. It operates at multiple layers.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The main characteristic of a multi-homed host is that is has multiple network interfaces, each connected to logically and physically separate networks. IP routing should be disabled to prevent the firewall from routing packets directly from one interface to the other. Source: FERREL, Robert G, questions and Answers for the CISSP Exam, domain 2 (derived from the Information Security Management Handbook, 4th Ed., by Tipton & Krause).

QUESTION 387
What is the main characteristic of a bastion host?

A. It is located on the internal network.
B. It is a hardened computer implementation
C. It is a firewall.
D. It does packet filtering.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: A bastion host is a special purpose computer on a network specifically designed and configured to withstand attack. The computer hosts a single application, for example a proxy server, and all other services are removed or limited to reduce the threat to the computer. It is hardened in this manner primarily due to its location and purpose, which is either on the outside of the firewall or in the DMZ and usually involves access from untrusted networks or computers.

http://en.wikipedia.org/wiki/Bastion_host

QUESTION 388
Which of the following statements pertaining to packet switching is incorrect?

A. Most data sent today uses digital signals over network employing packet switching.
B. Messages are divided into packets.
C. All packets from a message travel through the same route.
D. Each network node or point examines each packet for routing.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: When using packet switching, messages are broken down into packets. Source and destination address are added to each packet so that when passing through a network node, they can be examined and eventually rerouted through different paths as conditions change. All message packets may travel different paths and not arrive in the same order as sent. Packets need to be collected and reassembled into the original message at destination. Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 389
All hosts on an IP network have a logical ID called a(n):

A. IP address.
B. MAC address.
C. TCP address.

D. Datagram address.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: All hosts on a network have a logical ID that is called an IP address. An IP address is a numeric identifier that is assigned to each machine on an IP network. It designates the location of a device on a network. A MAC address is typically called a hardware address because it is "burned" into the NIC card. TCP address and Datagram address are imposter answers. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.

QUESTION 390
Each data packet is assigned the IP address of the sender and the IP address of the:

A. recipient.
B. host.
C. node.
D. network.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Each data packet is assigned the IP address of the sender and the IP address of the recipient. The term network refers to the part of the IP address that identifies each network. The terms host and node refer to the parts of the IP address that identify a specific machine on a network.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.

QUESTION 391
How long are IPv4 addresses?

A. 32 bits long.
B. 64 bits long.
C. 128 bits long.
D. 16 bits long.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: IPv4 addresses are currently 32 bits long. IPv6 addresses are 128 bits long. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.

QUESTION 392
Which of the following is used to find the Media Access Control address (MAC) that matches with a known Internet Protocol (IP) address?

A. Address Resolution Protocol (ARP).
B. Reverse Address Resolution Protocol (RARP).
C. Internet Control Message protocol (ICMP).
D. User Datagram Protocol (UDP).

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: ARP is used to find the Media Access Control address (MAC) that matches with a known Internet Protocol (IP) address.
The Address Resolution Protocol (ARP) is a computer networking protocol for determining a network host's link layer or hardware address when only its Internet Layer (IP) or Network Layer address is known
Reverse Address Resolution Protocol (RARP) is used to find the IP address that matches an Ethernet address.
ICMP is a management protocol and messaging service provider for IP (e.g. PING). UDP runs over IP. It is a best effort protocol that offers no reliability. UDS is used for application such as streaming media, voice over IP, the DNS protocol, as well as the Simple Network Management Protocol (SNMP).
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.
also see:
http://en.wikipedia.org/wiki/Address_resolution_protocol

QUESTION 393
Address Resolution Protocol (ARP) interrogates the network by sending out a?

A. broadcast.
B. multicast.
C. unicast.
D. semicast.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: ARP interrogates the network by sending out a broadcast seeking a network node that has a specific IP address, and asks it to reply with its hardware address. A broadcast message is sent to everyone whether or not the message was requested. A traditional unicast is a "one-to-one" or "narrowcast" message. A multicast is a "one-to-many" message that is traditionally only sent to those machine that requested the information. Semicast is an imposter answer. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.

QUESTION 394
When a station communicates on the network for the first time, which of the following protocol would search for and find the Internet Protocol (IP) address that matches with a known Ethernet address?

A. Address Resolution Protocol (ARP).
B. Reverse Address Resolution Protocol (RARP).
C. Internet Control Message protocol (ICMP).
D. User Datagram Protocol (UDP).

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The RARP protocol sends out a packet, which includes its MAC address and a request to be informed of the IP address that should be assigned to that MAC address. ARP does the opposite by broadcasting a request to find the Ethernet address that matches a known IP address.
ICMP supports packets containing error, control, and informational messages (e.g. PING). UDP runs over IP and is used primarily for broadcasting messages over a network. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.

QUESTION 395
Which of the following protocols' primary function is to send messages between network devices regarding the health of the network?

A. Reverse Address Resolution Protocol (RARP).
B. Address Resolution Protocol (ARP).
C. Internet Protocol (IP).
D. Internet Control Message protocol (ICMP).

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Its primary function is to send messages between network devices regarding the health of the network. ARP matches an IP address to an Ethernet address. RARP matches and Ethernet address to an IP address. ICMP runs on top of IP. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.

QUESTION 396
What is the primary reason why some sites choose not to implement Trivial File Transfer Protocol (TFTP)?

A. It is too complex to manage user access restrictions under TFTP
B. Due to the inherent security risks
C. It does not offer high level encryption like FTP
D. It cannot support the Lightwight Directory Access Protocol (LDAP)

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Some sites choose not to implement Trivial File Transfer Protocol (TFTP) due to the inherent security risks. TFTP is a UDP-based file transfer program that provides no security. There is no user authentication.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 88.

QUESTION 397
Why is Network File System (NFS) used?

A. It enables two different types of file systems to interoperate.
B. It enables two different types of file systems to share Sun applications.
C. It enables two different types of file systems to use IP/IPX.
D. It enables two different types of file systems to emulate each other.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Network File System (NFS) is a TCP/IP client/server application developed by Sun that enables different types of file systems to interoperate regardless of operating system or network architecture.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 88.

QUESTION 398
Which protocol is used to send email?

A. File Transfer Protocol (FTP).
B. Post Office Protocol (POP).
C. Network File System (NFS).
D. Simple Mail Transfer Protocol (SMTP).

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Simple Mail Transfer Protocol (SMTP) is a protocol for sending e-mail messages between servers. POP is a protocol used to retrieve e-mail from a mail server. NFS is a TCP/IP client/server application developed by Sun that enables different types of file systems to interoperate regardless of operating system or network architecture. FTP is the protocol that is used to facilitate file transfer between two machines. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 88.

QUESTION 399
What enables a workstation to boot without requiring a hard or floppy disk drive?

A. Bootstrap Protocol (BootP).
B. Reverse Address Resolution Protocol (RARP).
C. Address Resolution Protocol (ARP).
D. Classless Inter-Domain Routing (CIDR).

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Bootstrap Protocol (BootP) is an Internet Layer protocol that enables a workstation to boot without requiring a hard or floppy disk drive. Reverse Address Resolution Protocol (RARP) is a TCP/IP protocol that permits a physical address, such as an Ethernet address, to be translated into an IP address. Address Resolution Protocol (ARP) is a TCP/IP protocol that permits an IP address to be translated into a physical address. Classless Inter-Domain Routing (CIDR) is a new IP addressing scheme.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 88.

QUESTION 400
Which of the following protocols is designed to send individual messages securely?

A. Kerberos
B. Secure Electronic Transaction (SET).
C. Secure Sockets Layer (SSL).
D. Secure HTTP (S-HTTP).

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: An early standard for encrypting HTTP documents, Secure HTTP (S-HTTP) is designed to send individual messages securely. SSL is designed to establish a secure connection between two computers. SET was originated by VISA and MasterCard as an Internet credit card protocol using digital signatures. Kerberos is an authentication system. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 89.

QUESTION 401

Secure Electronic Transaction (SET) and Secure HTTP (S-HTTP) operate at which layer of the OSI model?

A. Application Layer.
B. Transport Layer.
C. Session Layer.
D. Network Layer.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The Secure Electronic Transaction (SET) and Secure HTTP (S-HTTP) operate at the Application Layer of the Open Systems Interconnect (OSI) model. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 89.

QUESTION 402
Which of the following is the core of fiber optic cables made of?

A. PVC
B. Glass fibers
C. Kevlar
D. Teflon

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Fiber optic cables have an outer insulating jacket made of Teflon or PVC, Kevlar fiber, which helps to strengthen the cable and prevent breakage, plastic coatings, used to cushion the fiber center. The center (core) of the cable is made of glass or plastic fibers. Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 3: Telecommunications and Network Security (page 31).

QUESTION 403
Which SSL version offers client-side authentication?

A. SSL v1
B. SSL v2
C. SSL v3
D. SSL v4

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Secure Sockets Layer (SSL) is the technology used in most Web-based applications. SSL version 2.0 supports strong authentication of the web server, but the authentication of the client side only comes with version 3.0. SSL v4 is not a defined standard. Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 3, Secured Connections to External Networks (page 54).

QUESTION 404
Which of the following statements pertaining to IPSec is incorrect?

A. IPSec can help in protecting networks from some of the IP network attacks.
B. IPSec provides confidentiality and integrity to information transferred over IP networks through transport

layer encryption and authentication.

C. IPSec protects against man-in-the-middle attacks.
D. IPSec protects against spoofing.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: IPSec provides confidentiality and integrity to information transferred over IP networks through network (not transport) layer encryption and authentication. All other statements are correct.
Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 6, Extranet Access Control Issues (page 110).

QUESTION 405
Which of the following is NOT a characteristic or shortcoming of packet filtering gateways?

A. The source and destination addresses, protocols, and ports contained in the IP packet header are the only information that is available to the router in making a decision whether or not to permit traffic access to an internal network.
B. They don't protect against IP or DNS address spoofing.
C. They do not support strong user authentication.
D. They are appropriate for medium-risk environment.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Packet filtering firewalls use routers with packet filtering rules to grant or deny access based on source address, destination address, and port. They offer minimum security but at a very low cost, and can be an appropriate choice for a low-risk environment.
Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 3, Secured Connections to External Networks (page 60).

QUESTION 406
In order to ensure the privacy and integrity of the data, connections between firewalls over public networks should use:

A. Screened subnets
B. Digital certificates
C. An encrypted Virtual Private Network
D. Encryption

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Virtual Private Networks allow a trusted network to communicate with another trusted network over untrusted networks such as the Internet. Screened Subnet: A screened subnet is essentially the same as the screened host architecture, but adds an extra strata of security by creating a network which the bastion host resides (often call perimeter network) which is separated from the internal network. A screened subnet will be deployed by adding a perimeter network in order to separate the internal network from the external. This assures that if there is a successful attack on the bastion host, the attacker is restricted to the perimeter network by the screening router that is connected between the internal and perimeter network.
Digital Certificates: Digital Certificates will be used in the intitial steps of establishing a VPN but they would not provide the encryption and integrity by themselves. Encryption: Even thou this seems like a choice that would include the other choices, encryption by itself does not provide integrity mechanims. So encryption would

satisfy only half of the requirements of the question.
Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 3, Secured Connections to External Networks (page 65).

QUESTION 407
Which of the following protocols does not operate at the data link layer (layer 2)?

A. PPP
B. RARP
C. L2F
D. ICMP

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: ICMP is the only of the mentioned protocols to operate at the network layer (layer 3). Other protocols operate at layer 2.
Source: WALLHOFF, John, CBK#2 Telecommunications and Network Security (CISSP Study Guide), April 2002 (page 1).

QUESTION 408
Which of the following protocols operates at the session layer (layer 5)?

A. RPC
B. IGMP
C. LPD
D. SPX

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Remotre Procedure Call (RPC) is the only of the above choices to operate at the session layer (layer 5).
All of the other answers were wrong.
LPD operates at layer 7
SPX operates at layer 4
IGMP operates at layer 3.
WALLHOFF, John, CBK#2 Telecommunications and Network Security (CISSP Study Guide), April 2002 (page 1).

QUESTION 409
Which layer of the TCP/IP protocol stack corresponds to the ISO/OSI Network layer (layer 3)?

A. Host-to-host layer
B. Internet layer
C. Network access layer
D. Session layer

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The Internet layer in the TCP/IP protocol stack corresponds to the network layer (layer 3) in the OSI/ISO model. The host-to-host layer corresponds to the transport layer (layer 4) in the OSI/ISO model. The

Network access layer corresponds to the data link and physical layers (layers 2 and 1) in the OSI/ISO model. The session layer is not defined in the TCP/IP protocol stack.
Source: WALLHOFF, John, CBK#2 Telecommunications and Network Security (CISSP Study Guide), April 2002 (page 1).

QUESTION 410
The concept of best effort delivery is best associated with?

A. TCP
B. HTTP
C. RSVP
D. IP

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The Internet Protocol (IP) is a data-oriented protocol used for communicating data across a packet-switched internetwork. IP provides an unreliable service (i.e., best effort delivery). This means that the network makes no guarantees about the packet. Low-level connectionless protocols such as DDP (under Appletalk) and IP usually provide besteffort delivery of data.
Best-effort delivery means that the protocol attempts to deliver any packets that meet certain requirements, such as containing a valid destination address, but the protocol does not inform the sender when it is unable to deliver the data, nor does it attempt to recover from error conditions and data loss.
Higher-level protocols such as TCP on the other hand, can provide reliable delivery of data. Reliable delivery includes error checking and recovery from error or loss of data. HTTP is the HyperText Transport Protocol used to establish connections to a web server and thus one of the higher level protocol using TCP to ensure delivery of all bytes between the client and the server. It was not a good choice according to the question presented.
Here is another definition from the TCP/IP guide at:
http://www.tcpipguide.com/free/t_IPOverviewandKeyOperationalCharacteristics.htm Delivered Unreliably: IP is said to be an "unreliable protocol". That doesn't mean that one day your IP software will decide to go fishing rather than run your network. J It does mean that when datagrams are sent from device A to device B, device A just sends each one and then moves on to the next. IP doesn't keep track of the ones it sent. It does not provide reliability or service quality capabilities such as error protection for the data it sends (though it does on the IP header), flow control or retransmission of lost datagrams.
For this reason, IP is sometimes called a best-effort protocol. It does what it can to get data to where it needs to go, but "makes no guarantees" that the data will actually get there.

QUESTION 411
Which layer of the OSI/ISO model handles physical addressing, network topology, line discipline, error notification, orderly delivery of frames, and optional flow control?

A. Physical
B. Data link
C. Network
D. Session

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The Data Link layer provides data transport across a physical link. It handles physical addressing, network topology, line discipline, error notification, orderly delivery of frames, and optional flow control.
Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 2, August 1999.

QUESTION 412

The Logical Link Control sub-layer is a part of which of the following?

A. The ISO/OSI Data Link layer
B. The Reference monitor
C. The Transport layer of the TCP/IP stack model
D. Change management control

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The OSI/ISO Data Link layer is made up of two sub-layers; (1) the Media Access Control layer refers downward to lower layer hardware functions and (2) the Logical Link Control refers upward to higher layer software functions. Other choices are distracters. Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 2, August 1999.

QUESTION 413
Which of the following services relies on UDP?

A. FTP
B. Telnet
C. DNS
D. SMTP

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: DNS relies on connectionless UDP whereas services like FTP, Telnet and SMTP rely on TCP. Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 2, August 1999.

QUESTION 414
How many bits of a MAC address uniquely identify a vendor, as provided by the IEEE?

A. 6 bits
B. 12 bits
C. 16 bits
D. 24 bits

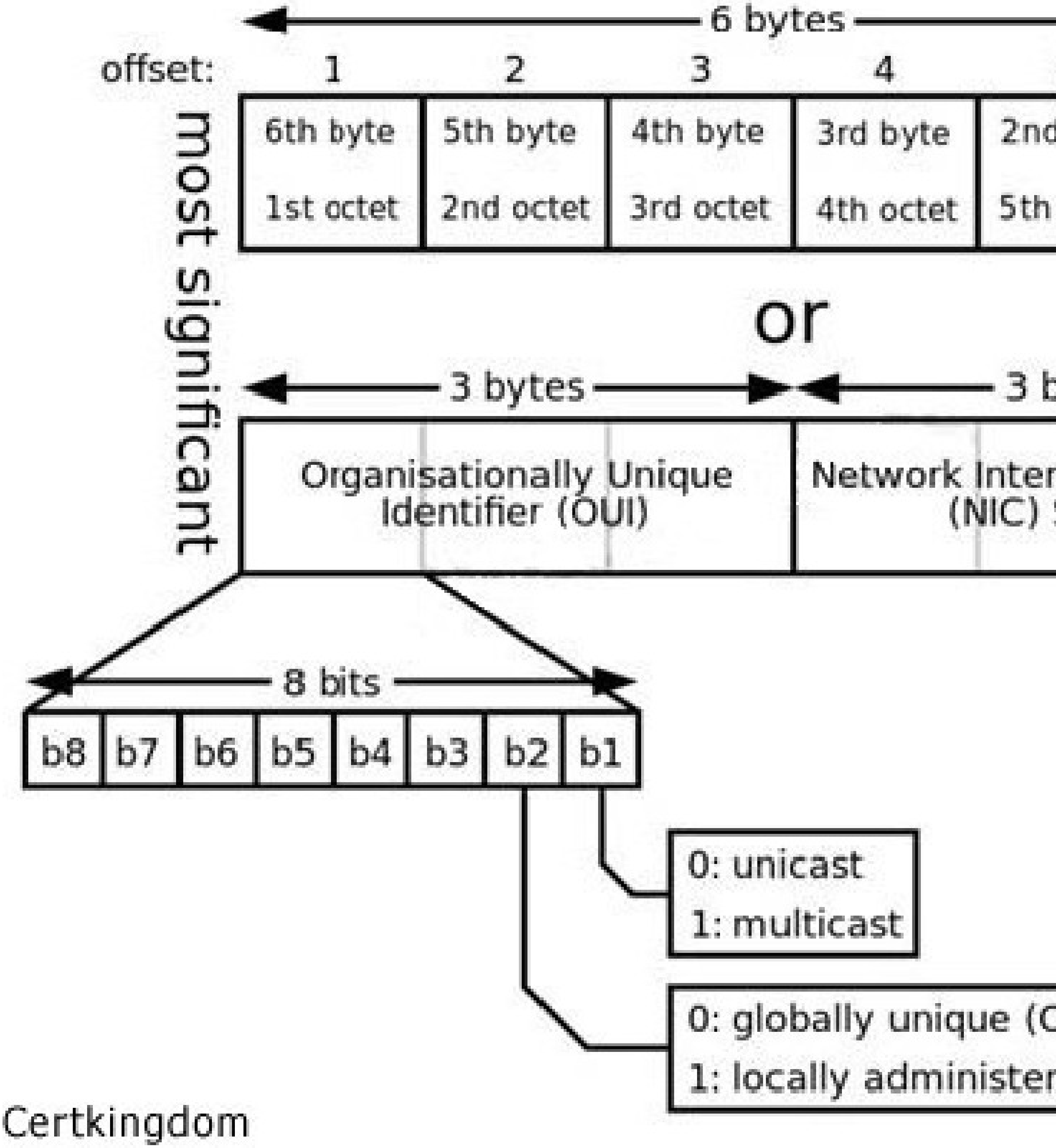
Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The MAC address is 48 bits long, 24 of which identify the vendor, as provided by the IEEE. The other 24 bits are provided by the vendor.
A media access control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used for numerous network technologies and most IEEE 802 network technologies, including Ethernet. Logically, MAC addresses are used in the media access control protocol sublayer of the OSI reference model.
MAC addresses are most often assigned by the manufacturer of a network interface card (NIC) and are stored in its hardware, such as the card's read-only memory or some other firmware mechanism. If assigned by the manufacturer, a MAC address usually encodes the manufacturer's registered identification number and may be referred to as the burned-in address. It may also be known as an Ethernet hardware address (EHA), hardware address or physical address. This is can be contrasted to a programmed address, where the host device issues commands to the NIC to use an arbitrary address. An example is many SOHO routers, where the ISP grants access to only one MAC address (used previously to inserting the router) so the router must

use that MAC address on its Internet-facing NIC. Therefore the router administrator configures a MAC address to override the burned-in one.

A network node may have multiple NICs and each must have one unique MAC address per NIC. See diagram below from Wikipedia showing the format of a MAC address. :

MAC Address format



Reference(s) used for this question:
http://en.wikipedia.org/wiki/MAC_address

QUESTION 415

Which Network Address Translation (NAT) is the most convenient and secure solution?

A. Hiding Network Address Translation
B. Port Address Translation
C. Dedicated Address Translation
D. Static Address Translation

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Static network address translation offers the most flexibility, but it is not normally practical given the shortage of IP version 4 addresses. Hiding network address translation is was an interim step in the development of network address translation technology, and is seldom used because port address translation offers additional features above and beyond those present in hiding network address translation while maintaining the same basic design and engineering considerations. PAT is often the most convenient and secure solution. Source: WACK, John et al., NIST Special publication 800-41, Guidelines on Firewalls and Firewall Policy, January 2002 (page 18).

QUESTION 416
What is the primary difference between FTP and TFTP?

A. Speed of negotiation
B. Authentication
C. Ability to automate
D. TFTP is used to transfer configuration files to and from network equipment.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: TFTP (Trivial File Transfer Protocol) is sometimes used to transfer configuration files from equipments such as routers but the primary difference between FTP and TFTP is that TFTP does not require authentication. Speed and ability to automate are not important. Both of these protocols (FTP and TFTP) can be used for transferring files across the Internet. The differences between the two protocols are explained below:
FTP is a complete, session-oriented, general purpose file transfer protocol. TFTP is used as a bare-bones special purpose file transfer protocol.
FTP can be used interactively. TFTP allows only unidirectional transfer of files. FTP depends on TCP, is connection oriented, and provides reliable control. TFTP depends on UDP, requires less overhead, and provides virtually no control.
FTP provides user authentication. TFTP does not.
FTP uses well-known TCP port numbers: 20 for data and 21 for connection dialog. TFTP uses UDP port number 69 for its file transfer activity.
The Windows NT FTP server service does not support TFTP because TFTP does not support authentication.
Windows 95 and TCP/IP-32 for Windows for Workgroups do not include a TFTP client program.
Ref: http://support.microsoft.com/kb/102737

QUESTION 417
In a SSL session between a client and a server, who is responsible for generating the master secret that will be used as a seed to generate the symmetric keys that will be used during the session?

A. Both client and server
B. The client's browser
C. The web server
D. The merchant's Certificate Server

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Once the merchant server has been authenticated by the browser client, the browser generates a master secret that is to be shared only between the server and client. This secret serves as a seed to generate the session (private) keys. The master secret is then encrypted with the merchant's public key and sent to the server. The fact that the master secret is generated by the client's browser provides the client assurance that the server is not reusing keys that would have been used in a previous session with another client. Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 6: Cryptography (page 112).
Also: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, page 569.

QUESTION 418
Which of the following statements pertaining to PPTP (Point-to-Point Tunneling Protocol) is incorrect?

A. PPTP allow the tunnelling of any protocols that can be carried within PPP.
B. PPTP does not provide strong encryption.
C. PPTP does not support any token-based authentication method for users.
D. PPTP is derived from L2TP.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: PPTP is an encapsulation protocol based on PPP that works at OSI layer 2 (Data Link) and that enables a single point-to-point connection, usually between a client and a server.
While PPTP depends on IP to establish its connection.
As currently implemented, PPTP encapsulates PPP packets using a modified version of the generic routing encapsulation (GRE) protocol, which gives PPTP to the flexibility of handling protocols other than IP, such as IPX and NETBEUI over IP networks.
PPTP does have some limitations:
It does not provide strong encryption for protecting data, nor does it support any token-based methods for authenticating users.
L2TP is derived from L2F and PPTP, not the opposite.

QUESTION 419
Which of the following is less likely to be used today in creating a Virtual Private Network?

A. L2TP
B. PPTP
C. IPSec
D. L2F

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: L2F (Layer 2 Forwarding) provides no authentication or encryption. It is a Protocol that supports the creation of secure virtual private dial-up networks over the Internet. At one point L2F was merged with PPTP to produce L2TP to be used on networks and not only on dial up links.
IPSec is now considered the best VPN solution for IP environments. Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 8: Cryptography (page 507).

QUESTION 420
Which of the following rules appearing in an Internet firewall policy is inappropriate?

A. Source routing shall be disabled on all firewalls and external routers.
B. Firewalls shall be configured to transparently allow all outbound and inbound services.
C. Firewalls should fail to a configuration that denies all services, and require a firewall administrator to re-enable services after a firewall has failed.
D. Firewalls shall not accept traffic on its external interfaces that appear to be coming from internal network addresses.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Unless approved by the Network Services manager, all in-bound services shall be intercepted and processed by the firewall. Allowing unrestricted services inbound and outbound is certainly NOT recommended and very dangerous.
Pay close attention to the keyword: all
All of the other choices presented are recommended practices for a firewall policy.
Reference(s) used for this question:
GUTTMAN, Barbara & BAGWILL, Robert, NIST Special Publication 800-xx, Internet Security Policy: A Technical Guide, Draft Version, May 25, 2000 (page 78).

QUESTION 421
SMTP can best be described as:

A. a host-to-host email protocol.
B. an email retrieval protocol.
C. a web-based e-mail reading protocol.
D. a standard defining the format of e-mail messages.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Simple Mail Transfer Protocol (SMTP) is a host-to-host email protocol. An SMTP server accepts email messages from other systems and stores them for the addressees. Stored email can be read in various ways. Users with interactive accounts on the email server machine can read the email using local email applications. Users on other systems can download their email via email clients using POP or IMAP email retrieval protocols. Sometimes mail can also be read through a web-based interface (using HTTP or HTTPS).
MIME is a standard defining the format of e-mail messages, as stated in RFC2045.
Source: GUTTMAN, Barbara & BAGWILL, Robert, NIST Special Publication 800-xx, Internet Security Policy: A Technical Guide, Draft Version, May 25, 2000 (pages 91-92).

QUESTION 422
What attack involves the perpetrator sending spoofed packet(s) wich contains the same destination and source IP address as the remote host, the same port for the source and destination, having the SYN flag, and targeting any open ports that are open on the remote host?

A. Boink attack
B. Land attack
C. Teardrop attack
D. Smurf attack

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: The Land attack involves the perpetrator sending spoofed packet(s) with the SYN flag set to the

victim's machine on any open port that is listening. The packet(s) contain the same destination and source IP address as the host, causing the victim's machine to reply to itself repeatedly. In addition, most systems experience a total freeze up, where as CTRL-ALT-DELETE fails to work, the mouse and keyboard become non operational and the only method of correction is to reboot via a reset button on the system or by turning the machine off. The Boink attack, a modified version of the original Teardrop and Bonk exploit programs, is very similar to the Bonk attack, in that it involves the perpetrator sending corrupt UDP packets to the host. It however allows the attacker to attack multiple ports where Bonk was mainly directed to port 53 (DNS).
The Teardrop attack involves the perpetrator sending overlapping packets to the victim, when their machine attempts to re-construct the packets the victim's machine hangs. A Smurf attack is a network-level attack against hosts where a perpetrator sends a large amount of ICMP echo (ping) traffic at broadcast addresses, all of it having a spoofed source address of a victim. If the routing device delivering traffic to those broadcast addresses performs the IP broadcast to layer 2 broadcast function, most hosts on that IP network will take the ICMP echo request and reply to it with an echo reply each, multiplying the traffic by the number of hosts responding. On a multi-access broadcast network, there could potentially be hundreds of machines to reply to each packet.
Resources:
http://en.wikipedia.org/wiki/Denial-of-service_attack
http://en.wikipedia.org/wiki/LAND

QUESTION 423
Which of the following firewall rules found on a firewall installed between an organization's internal network and the Internet would present the greatest danger to the internal network?

A. Permit all traffic between local hosts.
B. Permit all inbound ssh traffic.
C. Permit all inbound tcp connections.
D. Permit all syslog traffic to log-server.abc.org.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Any opening of an internal network to the Internet is susceptible of creating a new vulnerability. Of the given rules, the one that permits all inbound tcp connections is the less likely to be used since it amounts to almost having no firewall at all, tcp being widely used on the Internet.
Reference(s) used for this question:
ALLEN, Julia H., The CertKingdom to System and Network Security Practices, Addison-Wesley, 2001, Appendix B, Practice-Level Policy Considerations (page 409).

QUESTION 424
Which of the following statements pertaining to link encryption is false?

A. It encrypts all the data along a specific communication path.
B. It provides protection against packet sniffers and eavesdroppers.
C. Information stays encrypted from one end of its journey to the other.
D. User information, header, trailers, addresses and routing data that are part of the packets are encrypted.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: When using link encryption, packets have to be decrypted at each hop and encrypted again. Information staying encrypted from one end of its journey to the other is a characteristic of end-toend encryption, not link encryption.
Link Encryption vs. End-to-End Encryption
Link encryption encrypts the entire packet, including headers and trailers, and has to be decrypted at each hop.

End-to-end encryption does not encrypt the IP Protocol headers, and therefore does not need to be decrypted at each hop.
All in one, Page 735 & Glossary
and
Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 6).

QUESTION 425
Which of the following statements pertaining to packet filtering is incorrect?

A. It is based on ACLs.
B. It is not application dependant.
C. It operates at the network layer.
D. It keeps track of the state of a connection.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Packet filtering is used in the first generation of firewalls and does not keep track of the state of a connection. Stateful packet filtering does. Source: WALLHOFF, John, CISSP Summary 2002, April 2002, CBK#2 Telecommunications and Network Security (page 6)

QUESTION 426
Which of the following best defines source routing?

A. The packets hold the forwarding information so they don't need to let bridges and routers decide what is the best route or way to get to the destination.
B. The packets hold source information in a fashion that source address cannot be forged.
C. The packets are encapsulated to conceal source information.
D. The packets hold information about redundant paths in order to provide a higher reliability.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: With source routing, the packets hold the forwarding information so that they can find their way to the destination themselves without bridges and routers dictating their paths. In computer networking, source routing allows a sender of a packet to specify the route the packet takes through the network.
With source routing the entire path to the destination is known to the sender and is included when sending data. Source routing differs from most other routing in that the source makes most or all of the routing decisions for each router along the way.
Source:
WALLHOFF, John, CISSP Summary 2002, April 2002, CBK#2 Telecommunications and Network Security (page 5)
Wikipedia at http://en.wikipedia.org/wiki/Dynamic_Source_Routing

QUESTION 427
Which of the following is a method of multiplexing data where a communication channel is divided into an arbitrary number of variable bit-rate digital channels or data streams. This method allocates bandwidth dynamically to physical channels having information to transmit?

A. Time-division multiplexing
B. Asynchronous time-division multiplexing
C. Statistical multiplexing
D. Frequency division multiplexing

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Statistical multiplexing is a type of communication link sharing, very similar to dynamic bandwidth allocation (DBA). In statistical multiplexing, a communication channel is divided into an arbitrary number of variable bit-rate digital channels or data streams. The link sharing is adapted to the instantaneous traffic demands of the data streams that are transferred over each channel. This is an alternative to creating a fixed sharing of a link, such as in general time division multiplexing (TDM) and frequency division multiplexing (FDM). When performed correctly, statistical multiplexing can provide a link utilization improvement, called the statistical multiplexing gain.
Generally, the methods for multiplexing data include the following :
Time-division multiplexing (TDM): information from each data channel is allocated bandwidth based on pre-assigned time slots, regardless of whether there is data to transmit. Time-division multiplexing is used primarily for digital signals, but may be applied in analog multiplexing in which two or more signals or bit streams are transferred appearing simultaneously as sub-channels in one communication channel, but are physically taking turns on the channel. The time domain is divided into several recurrent time slots of fixed length, one for each sub-channel. A sample byte or data block of sub-channel 1 is transmitted during time slot 1, sub-channel 2 during time slot 2, etc. One TDM frame consists of one time slot per sub-channel plus a synchronization channel and sometimes error correction channel before the synchronization. After the last sub-channel, error correction, and synchronization, the cycle starts all over again with a new frame, starting with the second sample, byte or data block from sub-channel 1, etc. Asynchronous time-division multiplexing (ATDM): information from data channels is allocated bandwidth as needed, via dynamically assigned time slots. ATM provides functionality that is similar to both circuit switching and packet switching networks: ATM uses asynchronous timedivision multiplexing, and encodes data into small, fixed-sized packets (ISO-OSI frames) called cells. This differs from approaches such as the Internet Protocol or Ethernet that use variable sized packets and frames. ATM uses a connection-oriented model in which a virtual circuit must be established between two endpoints before the actual data exchange begins. These virtual circuits may be "permanent", i.e. dedicated connections that are usually preconfigured by the service provider, or "switched", i.e. set up on a per-call basis using signalling and disconnected when the call is terminated.
Frequency division multiplexing (FDM): information from each data channel is allocated bandwidth based on the signal frequency of the traffic. In telecommunications, frequency-division multiplexing (FDM) is a technique by which the total bandwidth available in a communication medium is divided into a series of non-overlapping frequency sub-bands, each of which is used to carry a separate signal. This allows a single transmission medium such as the radio spectrum, a cable or optical fiber to be shared by many signals.
Reference used for this question:
http://en.wikipedia.org/wiki/Statistical_multiplexing
and
http://en.wikipedia.org/wiki/Frequency_division_multiplexing and
Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 3: Technical Infrastructure and Operational Practices (page 114).

QUESTION 428
Which of the following is NOT a defined ISO basic task related to network management?

A. Fault management
B. Accounting resources
C. Security management
D. Communications management

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: ISO has defined five basic tasks related to network management :
Fault management: Detects the devices that present some kind of fault. Configuration management: Allows users to know, define and change remotely the configuration of any device.
Accounting resources: Holds the records of the resource usage in the WAN. Performance management:

Monitors usage levels and sets alarms when a threshold has been surpassed.
Security management: Detects suspicious traffic or users and generates alarms accordingly. Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 3: Technical Infrastructure and Operational Practices (page 137).

QUESTION 429
Why is infrared generally considered to be more secure to eavesdropping than multidirectional radio transmissions?

A. Because infrared eavesdropping requires more sophisticated equipment.
B. Because infrared operates only over short distances.
C. Because infrared requires direct line-of-sight paths.
D. Because infrared operates at extra-low frequencies (ELF).

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Infrared is generally considered to be more secure to eavesdropping than multidirectional radio transmissions because infrared requires direct line-of-sight paths. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 173).

QUESTION 430
Authentication Headers (AH) and Encapsulating Security Payload (ESP) protocols are the driving force of IPSec. Authentication Headers (AH) provides the following service except:

A. Authentication
B. Integrity
C. Replay resistance and non-repudiations
D. Confidentiality

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: AH provides integrity, authentication, and non-repudiation. AH does not provide encryption which means that NO confidentiality is in place if only AH is being used. You must make use of the Encasulating Security Payload if you wish to get confidentiality. IPSec uses two basic security protocols: Authentication Header (AH) and Encapsulation Security Payload.
AH is the authenticating protocol and the ESP is the authenticating and encrypting protocol that uses cryptographic mechanisms to provide source authentication, confidentiality and message integrity.
The modes of IPSEC, the protocols that have to be used are all negotiated using Security Association.
Security Associations (SAs) can be combined into bundles to provide authentication, confidentialility and layered communication.
Source:
TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, page 164.
also see:
Shon Harris, CISSP All In One Exam Guide, 5th Edition, Page 758

QUESTION 431
Encapsulating Security Payload (ESP) provides some of the services of Authentication Headers (AH), but it is primarily designed to provide:

A. Confidentiality

B. Cryptography
C. Digital signatures
D. Access Control

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, page 164.

QUESTION 432
Which of the following is NOT true about IPSec Tunnel mode?

A. Fundamentally an IP tunnel with encryption and authentication
B. Works at the Transport layer of the OSI model
C. Have two sets of IP headers
D. Established for gateway service

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: IPSec can be run in either tunnel mode or transport mode. Each of these modes has its own particular uses and care should be taken to ensure that the correct one is selected for the solution:
Tunnel mode is most commonly used between gateways, or at an end-station to a gateway, the gateway acting as a proxy for the hosts behind it.
Transport mode is used between end-stations or between an end-station and a gateway, if the gateway is being treated as a host--for example, an encrypted Telnet session from a workstation to a router, in which the router is the actual destination. As Figure 1 shows, basically transport mode should be used for end-to-end sessions and tunnel mode should be used for everything else. (Refer to the figure for the following discussion.)
Figure 1 Tunnel and transport modes in IPSec.
Figure 1 displays some examples of when to use tunnel versus transport mode:
Tunnel mode is most commonly used to encrypt traffic between secure IPSec gateways, such as between the Cisco router and PIX Firewall (as shown in example A in Figure 1). The IPSec gateways proxy IPSec for the devices behind them, such as Alice's PC and the HR servers in Figure 1. In example A, Alice connects to the HR servers securely through the IPSec tunnel set up between the gateways.
Tunnel mode is also used to connect an end-station running IPSec software, such as the Cisco Secure VPN Client, to an IPSec gateway, as shown in example B. In example C, tunnel mode is used to set up an IPSec tunnel between the Cisco router and a server running IPSec software. Note that Cisco IOS software and the PIX Firewall sets tunnel mode as the default IPSec mode.
Transport mode is used between end-stations supporting IPSec, or between an end-station and a gateway, if the gateway is being treated as a host. In example D, transport mode is used to set up an encrypted Telnet session from Alice's PC running Cisco Secure VPN Client software to terminate at the PIX Firewall, enabling Alice to remotely configure the PIX Firewall securely.
AH Tunnel Versus Transport Mode
Figure 2 shows the differences that the IPSec mode makes to AH. In transport mode, AH services protect the external IP header along with the data payload. AH services protect all the fields in the header that don't change in transport. The header goes after the IP header and before the ESP header, if present, and other higher-layer protocols.
In tunnel mode, the entire original header is authenticated, a new IP header is built, and the new IP header is protected in the same way as the IP header in transport mode.
Figure 2 AH tunnel versus transport mode.
AH is incompatible with Network Address Translation (NAT) because NAT changes the source IP address, which breaks the AH header and causes the packets to be rejected by the IPSec peer.
ESP Tunnel Versus Transport Mode
Figure 3 shows the differences that the IPSec mode makes to ESP. In transport mode, the IP payload is

encrypted and the original headers are left intact. The ESP header is inserted after the IP header and before the upper-layer protocol header. The upper-layer protocols are encrypted and authenticated along with the ESP header. ESP doesn't authenticate the IP header itself.

NOTE

Higher-layer information is not available because it's part of the encrypted payload. When ESP is used in tunnel mode, the original IP header is well protected because the entire original IP datagram is encrypted. With an ESP authentication mechanism, the original IP datagram and the ESP header are included; however, the new IP header is not included in the authentication.

When both authentication and encryption are selected, encryption is performed first, before authentication. One reason for this order of processing is that it facilitates rapid detection and rejection of replayed or bogus packets by the receiving node. Prior to decrypting the packet, the receiver can detect the problem and potentially reduce the impact of denial-of-service attacks.

Figure 3 ESP tunnel versus transport mode.

ESP can also provide packet authentication with an optional field for authentication. Cisco IOS software and the PIX Firewall refer to this service as ESP hashed message authentication code (HMAC). Authentication is calculated after the encryption is done. The current IPSec standard specifies SHA-1 and MD5 as the mandatory HMAC algorithms. The main difference between the authentication provided by ESP and AH is the extent of the coverage. Specifically, ESP doesn't protect any IP header fields unless those fields are encapsulated by ESP (tunnel mode). Figure 4 illustrates the fields protected by ESP HMAC.

Figure 4 ESP encryption with a keyed HMAC.

IPSec Transforms

An IPSec transform specifies a single IPSec security protocol (either AH or ESP) with its corresponding security algorithms and mode. Example transforms include the following:

The AH protocol with the HMAC with MD5 authentication algorithm in tunnel mode is used for authentication.

The ESP protocol with the triple DES (3DES) encryption algorithm in transport mode is used for confidentiality of data.

The ESP protocol with the 56-bit DES encryption algorithm and the HMAC with SHA-1 authentication algorithm in tunnel mode is used for authentication and confidentiality.

Transform Sets

A transform set is a combination of individual IPSec transforms designed to enact a specific security policy for traffic. During the ISAKMP IPSec security association negotiation that occurs in IKE phase 2 quick mode, the peers agree to use a particular transform set for protecting a particular data flow. Transform sets combine the following IPSec factors:

Mechanism for payload authentication--AH transform

Mechanism for payload encryption--ESP transform

IPSec mode (transport versus tunnel)

Transform sets equal a combination of an AH transform, plus an ESP transform, plus the IPSec mode (either tunnel or transport mode).

This brings us to the end of the second part of this five-part series of articles covering IPSec. Be sure to catch the next installment.

Cisco Press at: http://www.ciscopress.com/articles/printerfriendly.asp?p=25477 and

Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Pages 166-167.

QUESTION 433

Which of the following statements is NOT true of IPSec Transport mode?

A. It is required for gateways providing access to internal systems

B. Set-up when end-point is host or communications terminates at end-points

C. If used in gateway-to-host communication, gateway must act as host

D. When ESP is used for the security protocol, the hash is only applied to the upperlayer protocols contained in the packet

Correct Answer: A

Explanation

Explanation/Reference:

Explanation: Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th

Edition, Volume 2, 2001, CRC Press, NY, Pages 166-167.

QUESTION 434
All following observations about IPSec are correct except:

A. Default Hashing protocols are HMAC-MD5 or HMAC-SHA-1
B. Default Encryption protocol is Cipher Block Chaining mode DES, but other algorithms like ECC (Elliptic curve cryptosystem) can be used
C. Support two communication modes - Tunnel mode and Transport mode
D. Works only with Secret Key Cryptography

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Pages 166-167.

QUESTION 435
Which of the following statements pertaining to firewalls is incorrect?

A. Firewalls create bottlenecks between the internal and external network.
B. Firewalls allow for centralization of security services in machines optimized and dedicated to the task.
C. Firewalls protect a network at all layers of the OSI models.
D. Firewalls are used to create security checkpoints at the boundaries of private networks.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Firewalls can protect a network at multiple layers of the OSI models, however most of the firewalls do not have the ability to monitor the payload of the packets and see if an application level attack is taking place.
Today there are a new breed of firewall called Unified Threat Managers or UTM. They are a collection of products on a single computer and not necessarily a typical firewall. A UTM can address all of the layers but typically a firewall cannot. Firewalls are security checkpoints at the boundaries of internal networks through which every packet must pass and be inspected, hence they create bottlenecks between the internal and external networks. But since external connections are relatively slow compared to modern computers, the latency caused by this bottleneck can almost be transparent. By implementing the concept of border security, they centralize security services in machines optimized and dedicated to the task, thus relieving the other hosts on the network from that function.
Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 1: Understanding Firewalls.

QUESTION 436
Which of the following ports does NOT normally need to be open for a mail server to operate?

A. Port 110
B. Port 25
C. Port 119
D. Port 143

Correct Answer: C
Explanation

Explanation/Reference:

Explanation: Port 119 is normally used for the Network News Transfer Protocol. It is thus not need for a mail server, which would normally listen to ports 25 (SMTP), 110 (POP3) and 143 (IMAP).
Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 1: Understanding Firewalls.

QUESTION 437
Which of the following is an extension to Network Address Translation that permits multiple devices providing services on a local area network (LAN) to be mapped to a single public IP address?

A. IP Spoofing
B. IP subnetting
C. Port address translation
D. IP Distribution

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Port Address Translation (PAT), is an extension to network address translation (NAT) that permits multiple devices on a local area network (LAN) to be mapped to a single public IP address. The goal of PAT is to conserve IP addresses or to publish multiple hosts with service to the internet while having only one single IP assigned on the external side of your gateway. Most home networks use PAT. In such a scenario, the Internet Service Provider (ISP) assigns a single IP address to the home network's router. When Computer X logs on the Internet, the router assigns the client a port number, which is appended to the internal IP address. This, in effect, gives Computer X a unique address. If Computer Z logs on the Internet at the same time, the router assigns it the same local IP address with a different port number. Although both computers are sharing the same public IP address and accessing the Internet at the same time, the router knows exactly which computer to send specific packets to because each computer has a unique internal address.
Port Address Translation is also called porting, port overloading, port-level multiplexed NAT and single address NAT.
Shon Harris has the following example in her book:
The company owns and uses only one public IP address for all systems that need to communicate outside the internal network. How in the world could all computers use the exact same IP address? Good question. Here's an example: The NAT device has an IP address of 127.50.41.3. When computer A needs to communicate with a system on the Internet, the NAT device documents this computer's private address and source port number (10.10.44.3; port 43,887). The NAT device changes the IP address in the computer's packet header to 127.50.41.3, with the source port 40,000. When computer B also needs to communicate with a system on the Internet, the NAT device documents the private address and source port number (10.10.44.15; port 23,398) and changes the header information to 127.50.41.3 with source port 40,001. So when a system responds to computer A, the packet first goes to the NAT device, which looks up the port number 40,000 and sees that it maps to computer A's real information. So the NAT device changes the header information to address 10.10.44.3 and port 43,887 and sends it to computer A for processing. A company can save a lot more money by using PAT, because the company needs to buy only a few public IP addresses, which are used by all systems in the network.
As mentioned on Wikipedia:
NAT is also known as Port Address Translation: is a feature of a network device that translate TCP or UDP communications made between host on a private network and host on a public network. I allows a single public IP address to be used by many host on private network which is usually a local area network LAN
NAT effectively hides all TCP/IP-level information about internal hosts from the Internet.
The following were all inAnswer:
IP Spoofing - In computer networking, the term IP address spoofing or IP spoofing refers to the creation of Internet Protocol (IP) packets with a forged source IP address, called spoofing, with the purpose of concealing the identity of the sender or impersonating another computing system. Subnetting - Subnetting is a network design strategy that segregates a larger network into smaller components. While connected through the larger network, each subnetwork or subnet functions with a unique IP address. All systems that are assigned to a particular subnet will share values that are common for both the subnet and for the network as a whole. A different approach to network construction can be thought of as subnetting in reverse. Known as CIDR, or Classless Inter-Domain Routing, this approach also creates a series of subnetworks. Rather than dividing an

existing network into small components, CIDR takes smaller components and connects them into a larger network. This can often be the case when a business is acquired by a larger corporation. Instead of doing away with the network developed and used by the newly acquired business, the corporation chooses to continue operating that network as a subsidiary or an added component of the corporation's network. In effect, the system of the purchased entity becomes a subnet of the parent company's network.
IP Distribution - This is a generic term which could mean distribution of content over an IP network or distribution of IP addresses within a Company. Sometimes people will refer to this as Internet Protocol address management (IPAM) is a means of planning, tracking, and managing the Internet Protocol address space used in a network. Most commonly, tools such as DNS and DHCP are used in conjunction as integral functions of the IP address management function, and true IPAM glues these point services together so that each is aware of changes in the other (for instance DNS knowing of the IP address taken by a client via DHCP, and updating itself accordingly). Additional functionality, such as controlling reservations in DHCP as well as other data aggregation and reporting capability, is also common. IPAM tools are increasingly important as new IPv6 networks are deployed with larger address pools, different subnetting techniques, and more complex 128-bit hexadecimal numbers which are not as easily human-readable as IPv4 addresses.
Reference(s) used for this question:
STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 1:
Understanding Firewalls.
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition :
Telecommunications and Network Security, Page 350.
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 12765- 12774).
Telecommunications and Network Security, Page 604-606 http://searchnetworking.techtarget.com/definition/
Port-Address-Translation-PAT http://en.wikipedia.org/wiki/IP_address_spoofing
http://www.wisegeek.com/what-is-subnetting.htm
http://en.wikipedia.org/wiki/IP_address_management

QUESTION 438
At which OSI/ISO layer is an encrypted authentication between a client software package and a firewall performed?

A. Network layer
B. Session layer
C. Transport layer
D. Data link layer

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Encrypted authentication is a firewall feature that allows users on an external network to authenticate themselves to prove that they are authorized to access resources on the internal network. Encrypted authentication is convenient because it happens at the transport layer between a client software and a firewall, allowing all normal application software to run without hindrance.
Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 1:
Understanding Firewalls.

QUESTION 439
Which of the following is the primary reason why a user would choose a dial-up modem connection to the Internet when they have a faster, secure Internet connection through the organization's network?

A. To access web sites that blocked by the organization's proxy server.
B. To set up public services using the organization's resources.
C. To check their personal e-mail.
D. To circumvent the organization's security policy.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: All the choices above represent examples of circumventing the organization's security policy, which is the primary reason why a user would be using a dial-up Internet connection when a secure connection is available through the organization's network. Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 1:
Understanding Firewalls.

QUESTION 440
Which of the following can best eliminate dial-up access through a Remote Access Server as a hacking vector?

A. Using a TACACS+ server.
B. Installing the Remote Access Server outside the firewall and forcing legitimate users to authenticate to the firewall.
C. Setting modem ring count to at least 5.
D. Only attaching modems to non-networked hosts.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Containing the dial-up problem is conceptually easy: by installing the Remote Access Server outside the firewall and forcing legitimate users to authenticate to the firewall, any access to internal resources through the RAS can be filtered as would any other connection coming from the Internet.
The use of a TACACS+ Server by itself cannot eliminate hacking. Setting a modem ring count to 5 may help in defeating war-dialing hackers who look for modem by dialing long series of numbers.
Attaching modems only to non-networked hosts is not practical and would not prevent these hosts from being hacked.
Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 2:
Hackers.

QUESTION 441
Which of the following was designed to support multiple network types over the same serial link?

A. Ethernet
B. SLIP
C. PPP
D. PPTP

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: The Point-to-Point Protocol (PPP) was designed to support multiple network types over the same serial link, just as Ethernet supports multiple network types over the same LAN. PPP replaces the earlier Serial Line Internet Protocol (SLIP) that only supports IP over a serial link. PPTP is a tunneling protocol.
Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 3:
TCP/IP from a Security Viewpoint.

QUESTION 442
Before the advent of classless addressing, the address 128.192.168.16 would have been considered part of:

A. a class A network.
B. a class B network.
C. a class C network.

D. a class D network.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Before the advent of classless addressing, one could tell the size of a network by the first few bits of an IP address. If the first bit was set to zero (the first byte being from 0 to 127), the address was a class A network. Values from 128 to 191 were used for class B networks whereas values between 192 and 223 were used for class C networks. Class D, with values from 224 to 239 (the first three bits set to one and the fourth to zero), was reserved for IP multicast. Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 3:
TCP/IP from a Security Viewpoint.

QUESTION 443
What is an IP routing table?

A. A list of IP addresses and corresponding MAC addresses.
B. A list of station and network addresses with corresponding gateway IP address.
C. A list of host names and corresponding IP addresses.
D. A list of current network interfaces on which IP routing is enabled.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: A routing table is used when a destination IP address is not located on the current LAN segment. It consists of a list of station and network addresses and a corresponding gateway IP address further along to which a routing equipment should send packets that match that station or network address. A list of IP addresses and corresponding MAC addresses is an ARP table. A DNS is used to match host names and corresponding IP addresses. The last choice is a distracter. Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 3:
TCP/IP from a Security Viewpoint.

QUESTION 444
Which of the following was developed as a simple mechanism for allowing simple network terminals to load their operating system from a server over the LAN?

A. DHCP
B. BootP
C. DNS
D. ARP

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: BootP was developed as a simple mechanism for allowing simple network terminals to load their operating system from a server over the LAN. Over time, it has expanded to allow centralized configuration of many aspects of a host's identity and behavior on the network. Note that DHCP, more complex, has replaced BootP over time. Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 4:
Sockets and Services from a Security Viewpoint.

QUESTION 445
What is the greatest danger from DHCP?

A. An intruder on the network impersonating a DHCP server and thereby misconfiguring the DHCP clients.
B. Having multiple clients on the same LAN having the same IP address.
C. Having the wrong router used as the default gateway.
D. Having the organization's mail server unreachable.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The greatest danger from BootP or DHCP (Dynamic Host Control Protocol) is from an intruder on the network impersonating a DHCP server and thereby misconfiguring the DHCP clients. Other choices are possible consequences of DHCP impersonation. Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 4:
Sockets and Services from a Security Viewpoint.

QUESTION 446
Which of the following should NOT normally be allowed through a firewall?

A. SNMP
B. SMTP
C. HTTP
D. SSH

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The Simple Network Management Protocol (SNMP) is a useful tool for remotely managing network devices.
Since it can be used to reconfigure devices, SNMP traffic should be blocked at the organization's firewall.
Using a VPN with encryption or some type of Tunneling software would be highly recommended in this case.
Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 4:
Sockets and Services from a Security Viewpoint.

QUESTION 447
What can best be defined as a strongly protected computer that is in a network protected by a firewall (or is part of a firewall) and is the only host (or one of only a few hosts) in the network that can be directly accessed from networks on the other side of the firewall?

A. A bastion host
B. A screened subnet
C. A dual-homed host
D. A proxy server

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: The Internet Security Glossary (RFC2828) defines a bastion host as a strongly protected computer that is in a network protected by a firewall (or is part of a firewall) and is the only host (or one of only a few hosts) in the network that can be directly accessed from networks on the other side of the firewall.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 448
Which of the following can be defined as an Internet protocol by which a client workstation can dynamically access a mailbox on a server host to manipulate and retrieve mail messages that the server has received and

is holding for the client?

A. IMAP4
B. SMTP
C. MIME
D. PEM

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: RFC 2828 (Internet Security Glossary) defines the Internet Message Access Protocol, version 4 (IMAP4) as an Internet protocol by which a client workstation can dynamically access a mailbox on a server host to manipulate and retrieve mail messages that the server has received and is holding for the client.
IMAP4 has mechanisms for optionally authenticating a client to a server and providing other security services.
MIME is the MultiPurpose Internet Mail Extension. MIME extends the format of Internet mail to allow non-US-ASCII textual messages, non-textual messages, multipart message bodies, and non-US-ASCII information in message headers.
Simple Mail Transfer Protocol (SMTP) is a TCP-based, application-layer, Internet Standard protocol for moving electronic mail messages from one computer to another. Privacy Enhanced Mail (PEM) is an Internet protocol to provide data confidentiality, data integrity, and data origin authentication for electronic mail.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 449
Which of the following NAT firewall translation modes offers no protection from hacking attacks to an internal host using this functionality?

A. Network redundancy translation
B. Load balancing translation
C. Dynamic translation
D. Static translation

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Static translation (also called port forwarding), assigns a fixed address to a specific internal network resource (usually a server).
Static NAT is required to make internal hosts available for connection from external hosts. It merely replaces port information on a one-to-one basis. This affords no protection to statistically translated hosts: hacking attacks will be just as efficiently translated as any other valid connection attempt.
NOTE FROM CLEMENT:
Hiding Nat or Overloaded Nat is when you have a group of users behind a unique public IP address. This will provide you with some security through obscurity where an attacker scanning your network would see the unique IP address on the outside of the gateway but could not tell if there is one user, ten users, or hundreds of users behind that IP.
NAT was NEVER built as a security mechanism.
In the case of Static NAT used for some of your servers for example, your web server private IP is map to a valid external public IP on a one on one basis, your SMTP server private IP is mapped to a static public IP, and so on.
If an attacker scan the IP address range on the external side of the gateway he would discover every single one of your servers or any other hosts using static natting. Ports that are open, services that are listening, and all of this info could be gathered just as if the server was in fact using a public IP. It does not provide this security through obscurity mentioned above.
All of the other answer are incorrect.
Reference used for this question:
STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 7: Network Address

Translation.

QUESTION 450
Which of the following is the primary security feature of a proxy server?

A. Virus Detection
B. URL blocking
C. Route blocking
D. Content filtering

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: In many organizations, the HTTP proxy is used as a means to implement content filtering, for instance, by logging or blocking traffic that has been defined as, or is assumed to be nonbusiness related for some reason.
Although filtering on a proxy server or firewall as part of a layered defense can be quite effective to prevent, for instance, virus infections (though it should never be the only protection against viruses), it will be only moderately effective in preventing access to unauthorized services (such as certain remote-access services or file sharing), as well as preventing the download of unwanted content. HTTP Tunneling.
HTTP tunneling is technically a misuse of the protocol on the part of the designer of such tunneling applications. It has become a popular feature with the rise of the first streaming video and audio applications and has been implemented into many applications that have a market need to bypass user policy restrictions.
Usually, HTTP tunneling is applied by encapsulating outgoing traffic from an application in an HTTP request and incoming traffic in a response. This is usually not done to circumvent security, but rather, to be compatible with existing firewall rules and allow an application to function through a firewall without the need to apply special rules, or additional configurations.
The following are incorrect choices:
Virus Detection A proxy is not best at detection malware and viruses within content. A antivirus product would be use for that purpose.
URL blocking This would be a subset of Proxying, based on the content some URL's may be blocked by the proxy but it is not doing filtering based on URL addresses only. This is not the BEST answer.
Route blocking This is a function that would be done by Intrusion Detection and Intrusion prevention system and not the proxy. This could be done by filtering devices such as Firewalls and Routers as well. Again, not the best choice.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 6195-6201). Auerbach Publications. Kindle Edition.

QUESTION 451
In the context of network enumeration by an outside attacker and possible Distributed Denial of Service (DDoS) attacks, which of the following firewall rules is not appropriate to protect an organization's internal network?

A. Allow echo reply outbound
B. Allow echo request outbound
C. Drop echo request inbound
D. Allow echo reply inbound

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Echo replies outbound should be dropped, not allowed. There is no reason for any internet users to send ICMP ECHO Request to your interal hosts from the internet. If they wish to find out if a service is available, they can use a browser to connect to your web server or simply send an email if they wish to test

your mail service.
Echo replies outbound could be used as part of the SMURF amplification attack where someone will send ICMP echo requests to gateways broadcast addresses in order to amplify the request by X number of users sitting behind the gateway.
By allowing inbound echo requests and outbound echo replies, it makes it easier for attackers to learn about the internal network as well by performing a simply ping sweep. ICMP can also be used to find out which host has been up and running the longest which would indicates which patches are missing on the host if a critical patch required a reboot. ICMP can also be use for DDoS attacks, so you should strictly limit what type of ICMP traffic would be allowed to flow through your firewall.
On top of all this, tools such as LOKI could be use as a client-server application to transfer files back and forward between the internat and some of your internal hosts. LOKI is a client/server program published in the online publication Phrack . This program is a working proof-of-concept to demonstrate that data can be transmitted somewhat secretly across a network by hiding it in traffic that normally does not contain payloads. The example code can tunnel the equivalent of a Unix RCMD/RSH session in either ICMP echo request (ping) packets or UDP traffic to the DNS port. This is used as a back door into a Unix system after root access has been compromised. Presence of LOKI on a system is evidence that the system has been compromised in the past. The outbound echo request and inbound echo reply allow internal users to verify connectivity with external hosts.
The following answers are incorrect:
Allow echo request outbound The outbound echo request and inbound echo reply allow internal users to verify connectivity with external hosts.
Drop echo request inbound There is no need for anyone on the internet to attempt pinging your internal hosts.
Allow echo reply inbound The outbound echo request and inbound echo reply allow internal users to verify connectivity with external hosts.
Reference(s) used for this question:
http://www.phrack.org/issues.html?issue=49&id=6
STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 10: The Perfect Firewall.

QUESTION 452
Which of the following packets should NOT be dropped at a firewall protecting an organization's internal network?

A. Inbound packets with Source Routing option set
B. Router information exchange protocols
C. Inbound packets with an internal address as the source IP address
D. Outbound packets with an external destination IP address

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Normal outbound traffic has an internal source IP address and an external destination IP address. Traffic with an internal source IP address should only come from an internal interface. Such packets coming from an external interface should be dropped. Packets with the source-routing option enabled usually indicates a network intrusion attempt. Router information exchange protocols like RIP and OSPF should be dropped to avoid having internal routing equipment being reconfigured by external agents. Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 10:
The Perfect Firewall.

QUESTION 453
Why does fiber optic communication technology have significant security advantage over other transmission technology?

A. Higher data rates can be transmitted.
B. Interception of data traffic is more difficult.
C. Traffic analysis is prevented by multiplexing.
D. Single and double-bit errors are correctable.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: It would be correct to select the first answer if the world "security" was not in the question.
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 454
Layer 4 of the OSI stack is known as:

A. the data link layer
B. the transport layer
C. the network layer
D. the presentation layer

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 455
Another name for a VPN is a:

A. tunnel
B. one-time password
C. pipeline
D. bypass

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 456
Why is traffic across a packet switched network difficult to monitor?

A. Packets are link encrypted by the carrier
B. Government regulations forbids monitoring
C. Packets can take multiple paths when transmitted
D. The network factor is too high

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: With a packet switched network, packets are difficult to monitor because they can be transmitted using different paths.
A packet-switched network is a digital communications network that groups all transmitted data, irrespective of content, type, or structure into suitably sized blocks, called packets. The network over which packets are transmitted is a shared network which routes each packet independently from all others and allocates transmission resources as needed. The principal goals of packet switching are to optimize utilization of available link capacity, minimize response times and increase the robustness of communication. When traversing network adapters, switches and other network nodes, packets are buffered and queued, resulting in

variable delay and throughput, depending on the traffic load in the network. Most modern Wide Area Network (WAN) protocols, including TCP/IP, X.25, and Frame Relay, are based on packet-switching technologies. In contrast, normal telephone service is based on a circuit-switching technology, in which a dedicated line is allocated for transmission between two parties. Circuit-switching is ideal when data must be transmitted quickly and must arrive in the same order in which it's sent. This is the case with most real-time data, such as live audio and video. Packet switching is more efficient and robust for data that can withstand some delays in transmission, such as e-mail messages and Web pages.
All of the other answer are wrong
Reference(s) used for this question:
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.
and
https://en.wikipedia.org/wiki/Packet-switched_network
and
http://www.webopedia.com/TERM/P/packet_switching.html

QUESTION 457
Which one of the following is used to provide authentication and confidentiality for e-mail messages?

A. Digital signature

B. PGP

C. IPSEC AH

D. MD4

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: Instead of using a Certificate Authority, PGP uses a "Web of Trust", where users can certify each other in a mesh model, which is best applied to smaller groups. In cryptography, a web of trust is a concept used in PGP, GnuPG, and other OpenPGP compatible systems to establish the authenticity of the binding between a public key and its owner. Its decentralized trust model is an alternative to the centralized trust model of a public key infrastructure (PKI), which relies exclusively on a certificate authority (or a hierarchy of such). The web of trust concept was first put forth by PGP creator Phil Zimmermann in 1992 in the manual for PGP version 2.0.
Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting and decrypting texts, E-mails, files, directories and whole disk partitions to increase the security of e-mail communications. It was created by Phil Zimmermann in 1991.
As per Shon Harris's book:
Pretty Good Privacy (PGP) was designed by Phil Zimmerman as a freeware e-mail security program and was released in 1991. It was the first widespread public key encryption program. PGP is a complete cryptosystem that uses cryptographic protection to protect e-mail and files. It can use RSA public key encryption for key management and use IDEA symmetric cipher for bulk encryption of data, although the user has the option of picking different types of algorithms for these functions. PGP can provide confidentiality by using the IDEA encryption algorithm, integrity by using the MD5 hashing algorithm, authentication by using the public key certificates, and nonrepudiation by using cryptographically signed messages. PGP initially used its own type of digital certificates rather than what is used in PKI, but they both have similar purposes. Today PGP support X.509 V3 digital certificates.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 169).
Shon Harris, CISSP All in One book
https://en.wikipedia.org/wiki/Pretty_Good_Privacy
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 458
What is a packet sniffer?

A. It tracks network connections to off-site locations.
B. It monitors network traffic for illegal packets.
C. It scans network segments for cabling faults.
D. It captures network traffic for later analysis.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 459
Which of the following media is MOST resistant to EMI interference?

A. microwave
B. fiber optic
C. twisted pair
D. coaxial cable

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: A fiber optic cable is a physical medium that is capable of conducting modulated light trasmission. Fiber optic cable carries signals as light waves, thus creating higher trasmission speeds and greater distances due to less attenuation. This type of cabling is more difficult to tap than other cabling and is most resistant to interference, especially EMI. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 103).

QUESTION 460
At which layer of ISO/OSI does the fiber optics work?

A. Network layer
B. Transport layer
C. Data link layer
D. Physical layer

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: The
Answer: Physical layer The Physical layer is responsible for the transmission of the data through the physical medium. This includes such things as cables. Fiber optics is a cabling mechanism which works at Physical layer of OSI model All of the other answers are incorrect.
The following reference(s) were/was used to create this question:
Shon Harris all in one - Chapter 7 (Cabling)

QUESTION 461
While using IPsec, the ESP and AH protocols both provides integrity services. However when using AH, some special attention needs to be paid if one of the peers uses NAT for address translation service. Which of the items below would affects the use of AH and it´s Integrity Check Value (ICV) the most?

A. Key session exchange

B. Packet Header Source or Destination address
C. VPN cryptographic key size
D. Crypotographic algorithm used

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: It may seem odd to have two different protocols that provide overlapping functionality.
AH provides authentication and integrity, and ESP can provide those two functions and confidentiality.
Why even bother with AH then?
In most cases, the reason has to do with whether the environment is using network address translation (NAT). IPSec will generate an integrity check value (ICV), which is really the same thing as a MAC value, over a portion of the packet. Remember that the sender and receiver generate their own values. In IPSec, it is called an ICV value. The receiver compares her ICV value with the one sent by the sender. If the values match, the receiver can be assured the packet has not been modified during transmission. If the values are different, the packet has been altered and the receiver discards the packet.
The AH protocol calculates this ICV over the data payload, transport, and network headers. If the packet then goes through a NAT device, the NAT device changes the IP address of the packet. That is its job. This means a portion of the data (network header) that was included to calculate the ICV value has now changed, and the receiver will generate an ICV value that is different from the one sent with the packet, which means the packet will be discarded automatically. The ESP protocol follows similar steps, except it does not include the network header portion when calculating its ICV value. When the NAT device changes the IP address, it will not affect the receiver's ICV value because it does not include the network header when calculating the ICV. Here is a tutorial on IPSEC from the Shon Harris Blog:
The Internet Protocol Security (IPSec) protocol suite provides a method of setting up a secure channel for protected data exchange between two devices. The devices that share this secure channel can be two servers, two routers, a workstation and a server, or two gateways between different networks. IPSec is a widely accepted standard for providing network layer protection. It can be more flexible and less expensive than end-to end and link encryption methods. IPSec has strong encryption and authentication methods, and although it can be used to enable tunneled communication between two computers, it is usually employed to establish virtual private networks (VPNs) among networks across the Internet.
IPSec is not a strict protocol that dictates the type of algorithm, keys, and authentication method to use. Rather, it is an open, modular framework that provides a lot of flexibility for companies when they choose to use this type of technology. IPSec uses two basic security protocols:
Authentication Header (AH) and Encapsulating Security Payload (ESP). AH is the authenticating protocol, and ESP is an authenticating and encrypting protocol that uses cryptographic mechanisms to provide source authentication, confidentiality, and message integrity. IPSec can work in one of two modes: transport mode, in which the payload of the message is protected, and tunnel mode, in which the payload and the routing and header information are protected. ESP in transport mode encrypts the actual message information so it cannot be sniffed and uncovered by an unauthorized entity. Tunnel mode provides a higher level of protection by also protecting the header and trailer data an attacker may find useful. Figure 8-26 shows the high-level view of the steps of setting up an IPSec connection. Each device will have at least one security association (SA) for each VPN it uses. The SA, which is critical to the IPSec architecture, is a record of the configurations the device needs to support an IPSec connection. When two devices complete their handshaking process, which means they have agreed upon a long list of parameters they will use to communicate, these data must be recorded and stored somewhere, which is in the SA.
The SA can contain the authentication and encryption keys, the agreed-upon algorithms, the key lifetime, and the source IP address. When a device receives a packet via the IPSec protocol, it is the SA that tells the device what to do with the packet. So if device B receives a packet from device C via IPSec, device B will look to the corresponding SA to tell it how to decrypt the packet, how to properly authenticate the source of the packet, which key to use, and how to reply to the message if necessary.
SAs are directional, so a device will have one SA for outbound traffic and a different SA for inbound traffic for each individual communication channel. If a device is connecting to three devices, it will have at least six SAs, one for each inbound and outbound connection per remote device. So how can a device keep all of these SAs organized and ensure that the right SA is invoked for the right connection? With the mighty secu rity parameter index (SPI), that's how. Each device has an SPI that keeps track of the different SAs and tells the device which one is appropriate to invoke for the different packets it receives. The SPI value is in the header of an IPSec

packet, and the device reads this value to tell it which SA to consult. IPSec can authenticate the sending devices of the packet by using MAC (covered in the earlier section, "The One-Way Hash"). The ESP protocol can provide authentication, integrity, and confidentiality if the devices are configured for this type of functionality. So if a company just needs to make sure it knows the source of the sender and must be assured of the integrity of the packets, it would choose to use AH. If the company would like to use these services and also have confidentiality, it would use the ESP protocol because it provides encryption functionality. In most cases, the reason ESP is employed is because the company must set up a secure VPN connection.

It may seem odd to have two different protocols that provide overlapping functionality. AH provides authentication and integrity, and ESP can provide those two functions and confidentiality. Why even bother with AH then? In most cases, the reason has to do with whether the environment is using network address translation (NAT). IPSec will generate an integrity check value (ICV), which is really the same thing as a MAC value, over a portion of the packet. Remember that the sender and receiver generate their own values. In IPSec, it is called an ICV value. The receiver compares her ICV value with the one sent by the sender. If the values match, the receiver can be assured the packet has not been modified during transmission. If the values are different, the packet has been altered and the receiver discards the packet.

The AH protocol calculates this ICV over the data payload, transport, and network headers. If the packet then goes through a NAT device, the NAT device changes the IP address of the packet. That is its job. This means a portion of the data (network header) that was included to calculate the ICV value has now changed, and the receiver will generate an ICV value that is different from the one sent with the packet, which means the packet will be discarded automatically. The ESP protocol follows similar steps, except it does not include the network header portion when calculating its ICV value. When the NAT device changes the IP address, it will not affect the receiver's ICV value because it does not include the network header when calculating the ICV. Because IPSec is a framework, it does not dictate which hashing and encryption algorithms are to be used or how keys are to be exchanged between devices. Key management can be handled manually or automated by a key management protocol. The de facto standard for IPSec is to use Internet Key Exchange (IKE), which is a combination of the ISAKMP and OAKLEY protocols. The Internet Security Association and Key Management Protocol (ISAKMP) is a key exchange architecture that is independent of the type of keying mechanisms used. Basically, ISAKMP provides the framework of what can be negotiated to set up an IPSec connection (algorithms, protocols, modes, keys). The OAKLEY protocol is the one that carries out the negotiation process. You can think of ISAKMP as providing the playing field (the infrastructure) and OAKLEY as the guy running up and down the playing field (carrying out the steps of the negotiation). IPSec is very complex with all of its components and possible configurations. This complexity is what provides for a great degree of flexibility, because a company has many different configuration choices to achieve just the right level of protection. If this is all new to you and still confusing, please review one or more of the following references to help fill in the gray areas.

The following answers are incorrect:

The other options are distractors.

The following reference(s) were/was used to create this question:

Shon Harris, CISSP All-in-One Exam Guide- fiveth edition, page 759 and
https://neodean.wordpress.com/tag/security-protocol/

QUESTION 462

Which of the following service is a distributed database that translate host name to IP address to IP address to host name?

A. DNS

B. FTP

C. SSH

D. SMTP

Correct Answer: A

Explanation

Explanation/Reference:

Explanation: The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates information from domain names with each of the assigned entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for locating computer services and devices worldwide. The Domain Name

System is an essential component of the functionality of the Internet. This article presents a functional description of the Domain Name System.

For your exam you should know below information general Internet terminology:

Network access point - Internet service providers access internet using net access point.A Network Access Point (NAP) was a public network exchange facility where Internet service providers (ISPs) connected with one another in peering arrangements. The NAPs were a key component in the transition from the 1990s NSFNET era (when many networks were government sponsored and commercial traffic was prohibited) to the commercial Internet providers of today. They were often points of considerable Internet congestion. Internet Service Provider (ISP) - An Internet service provider (ISP) is an organization that provides services for accessing, using, or participating in the Internet. Internet service providers may be organized in various forms, such as commercial, community-owned, non-profit, or otherwise privately owned. Internet services typically provided by ISPs include Internet access, Internet transit, domain name registration, web hosting, co-location.

Telnet or Remote Terminal Control Protocol -A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network. To start a Telnet session, you must log in to a server by entering a valid username and password. Telnet is a common way to remotely control Web servers.

Internet Link- Internet link is a connection between Internet users and the Internet service provider. Secure Shell or Secure Socket Shell (SSH) - Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three utilities - slogin, ssh, and scp - that are secure versions of the earlier UNIX utilities, rlogin, rsh, and rcp. SSH commands are encrypted and secure in several ways. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted. Domain Name System (DNS) - The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates information from domain names with each of the assigned entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for locating computer services and devices worldwide. The Domain Name System is an essential component of the functionality of the Internet. This article presents a functional description of the Domain Name System.

File Transfer Protocol (FTP) - The File Transfer Protocol or FTP is a client/server application that is used to move files from one system to another. The client connects to the FTP server, authenticates and is given access that the server is configured to permit. FTP servers can also be configured to allow anonymous access by logging in with an email address but no password. Once connected, the client may move around between directories with commands available Simple Mail Transport Protocol (SMTP) - SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail. On Unix-based systems, send mail is the most widely-used SMTP server for e-mail. A commercial package, Send mail, includes a POP3 server. Microsoft Exchange includes an SMTP server and can also be set up to include POP3 support.

The following answers are incorrect:

SMTP - Simple Mail Transport Protocol (SMTP) - SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail. On Unix-based systems, send mail is the most widelyused SMTP server for e-mail. A commercial package, Send mail, includes a POP3 server. Microsoft Exchange includes an SMTP server and can also be set up to include POP3 support. FTP - The File Transfer Protocol or FTP is a client/server application that is used to move files from one system to another. The client connects to the FTP server, authenticates and is given access that the server is configured to permit. FTP servers can also be configured to allow anonymous access by logging in with an email address but no password. Once connected, the client may move around between directories with commands available SSH - Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three utilities - slogin, ssh, and scp - that are secure versions of the earlier UNIX utilities, rlogin, rsh, and rcp. SSH commands

are encrypted and secure in several ways. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.
The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 273 and 274

QUESTION 463
In computing what is the name of a non-self-replicating type of malware program containing malicious code that appears to have some useful purpose but also contains code that has a malicious or harmful purpose imbedded in it, when executed, carries out actions that are unknown to the person installing it, typically causing loss or theft of data, and possible system harm.

A. virus
B. worm
C. Trojan horse.
D. trapdoor

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: A trojan horse is any code that appears to have some useful purpose but also contains code that has a malicious or harmful purpose imbedded in it. A Trojan often also includes a trapdoor as a means to gain access to a computer system bypassing security controls.
Wikipedia defines it as:
A Trojan horse, or Trojan, in computing is a non-self-replicating type of malware program containing malicious code that, when executed, carries out actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm. The term is derived from the story of the wooden horse used to trick defenders of Troy into taking concealed warriors into their city in ancient Greece, because computer Trojans often employ a form of social engineering, presenting themselves as routine, useful, or interesting in order to persuade victims to install them on their computers.
The following answers are incorrect:
virus. Is incorrect because a Virus is a malicious program and is does not appear to be harmless, it's sole purpose is malicious intent often doing damage to a system. A computer virus is a type of malware that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected".
worm. Is incorrect because a Worm is similiar to a Virus but does not require user intervention to execute. Rather than doing damage to the system, worms tend to self-propagate and devour the resources of a system. A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.
trapdoor. Is incorrect because a trapdoor is a means to bypass security by hiding an entry point into a system. Trojan Horses often have a trapdoor imbedded in them.

http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29 and
http://en.wikipedia.org/wiki/Computer_virus
and
http://en.wikipedia.org/wiki/Computer_worm
and
http://en.wikipedia.org/wiki/Backdoor_%28computing%29

QUESTION 464
Which of the following virus types changes some of its characteristics as it spreads?

A. Boot Sector
B. Parasitic

C. Stealth
D. Polymorphic

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: A Polymorphic virus produces varied but operational copies of itself in hopes of evading anti-virus software.
The following answers are incorrect:
boot sector. Is incorrect because it is not the best answer. A boot sector virus attacks the boot sector of a drive. It describes the type of attack of the virus and not the characteristics of its composition.
parasitic. Is incorrect because it is not the best answer. A parasitic virus attaches itself to other files but does not change its characteristics.
stealth. Is incorrect because it is not the best answer. A stealth virus attempts to hide changes of the affected files but not itself.

QUESTION 465
Virus scanning and content inspection of SMIME encrypted e-mail without doing any further processing is:

A. Not possible
B. Only possible with key recovery scheme of all user keys
C. It is possible only if X509 Version 3 certificates are used
D. It is possible only by "brute force" decryption

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Content security measures presumes that the content is available in cleartext on the central mail server.
Encrypted emails have to be decrypted before it can be filtered (e.g. to detect viruses), so you need the decryption key on the central "crypto mail server". There are several ways for such key management, e.g. by message or key recovery methods. However, that would certainly require further processing in order to achieve such goal.

QUESTION 466
Which virus category has the capability of changing its own code, making it harder to detect by anti-virus software?

A. Stealth viruses
B. Polymorphic viruses
C. Trojan horses
D. Logic bombs

Correct Answer: B
Explanation

Explanation/Reference:
Explanation: A polymorphic virus has the capability of changing its own code, enabling it to have many different variants, making it harder to detect by anti-virus software. The particularity of a stealth virus is that it tries to hide its presence after infecting a system. A Trojan horse is a set of unauthorized instructions that are added to or replacing a legitimate program. A logic bomb is a set of instructions that is initiated when a specific event occurs. Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 11: Application and System Development (page 786).

QUESTION 467
The high availability of multiple all-inclusive, easy-to-use hacking tools that do NOT require much technical knowledge has brought a growth in the number of which type of attackers?

A. Black hats
B. White hats
C. Script kiddies
D. Phreakers

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: As script kiddies are low to moderately skilled hackers using available scripts and tools to easily launch attacks against victims.
The other answers are incorrect because :
Black hats is incorrect as they are malicious , skilled hackers. White hats is incorrect as they are security professionals. Phreakers is incorrect as they are telephone/PBX (private branch exchange) hackers.
Reference : Shon Harris AIO v3 , Chapter 12: Operations security , Page : 830

QUESTION 468
Which of the following computer crime is MORE often associated with INSIDERS?

A. IP spoofing
B. Password sniffing
C. Data diddling
D. Denial of service (DOS)

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: It refers to the alteration of the existing data , most often seen before it is entered into an application.This type of crime is extremely common and can be prevented by using appropriate access controls and proper segregation of duties. It will more likely be perpetrated by insiders, who have access to data before it is processed.
The other answers are incorrect because :
IP Spoofing is not correct as the questions asks about the crime associated with the insiders.
Spoofing is generally accomplished from the outside.
Password sniffing is also not the BEST answer as it requires a lot of technical knowledge in understanding the encryption and decryption process.
Denial of service (DOS) is also incorrect as most Denial of service attacks occur over the internet. Reference : Shon Harris , AIO v3 , Chapter-10 : Law , Investigation & Ethics , Page : 758-760.

QUESTION 469
What do the ILOVEYOU and Melissa virus attacks have in common?

A. They are both denial-of-service (DOS) attacks.
B. They have nothing in common.
C. They are both masquerading attacks.
D. They are both social engineering attacks.

Correct Answer: C
Explanation

Explanation/Reference:

Explanation: While a masquerading attack can be considered a type of social engineering, the Melissa and ILOVEYOU viruses are examples of masquerading attacks, even if it may cause some kind of denial of service due to the web server being flooded with messages. In this case, the receiver confidently opens a message coming from a trusted individual, only to find that the message was sent using the trusted party's identity.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 10: Law, Investigation, and Ethics (page 650).

QUESTION 470
Crackers today are MOST often motivated by their desire to:

A. Help the community in securing their networks.
B. Seeing how far their skills will take them.
C. Getting recognition for their actions.
D. Gaining Money or Financial Gains.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: A few years ago the best choice for this question would have been seeing how far their skills can take them. Today this has changed greatly, most crimes committed are financially motivated.
Profit is the most widespread motive behind all cybercrimes and, indeed, most crimes- everyone wants to make money. Hacking for money or for free services includes a smorgasbord of crimes such as embezzlement, corporate espionage and being a "hacker for hire". Scams are easier to undertake but the likelihood of success is much lower. Money-seekers come from any lifestyle but those with persuasive skills make better con artists in the same way as those who are exceptionally tech-savvy make better "hacks for hire". "White hats" are the security specialists (as opposed to Black Hats) interested in helping the community in securing their networks. They will test systems and network with the owner authorization.
A Black Hat is someone who uses his skills for offensive purpose. They do not seek authorization before they attempt to comprise the security mechanisms in place. "Grey Hats" are people who sometimes work as a White hat and other times they will work as a "Black Hat", they have not made up their mind yet as to which side they prefer to be.
The following are incorrect answers:
All the other choices could be possible reasons but the best one today is really for financial gains.
References used for this question:
http://library.thinkquest.org/04oct/00460/crimeMotives.html and
http://www.informit.com/articles/article.aspx?p=1160835 and
http://www.aic.gov.au/documents/1/B/A/%7B1BA0F612-613A-494D-B6C5- 06938FE8BB53%7Dhtcb006.pdf

QUESTION 471
What best describes a scenario when an employee has been shaving off pennies from multiple accounts and depositing the funds into his own bank account?

A. Data fiddling
B. Data diddling
C. Salami techniques
D. Trojan horses

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2001, Page 644.

QUESTION 472
Java is not:

A. Object-oriented.

B. Distributed.

C. Architecture Specific.

D. Multithreaded.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation: JAVA was developed so that the same program could be executed on multiple hardware and operating system platforms, it is not Architecture Specific.
The following answers are incorrect:
Object-oriented. Is not correct because JAVA is object-oriented. It should use the object-oriented programming methodology.
Distributed. Is incorrect because JAVA was developed to be able to be distrubuted, run on multiple computer systems over a network.
Multithreaded. Is incorrect because JAVA is multi-threaded that is calls to subroutines as is the case with object-oriented programming.
A virus is a program that can replicate itself on a system but not necessarily spread itself by network connections.

QUESTION 473
What is malware that can spread itself over open network connections?

A. Worm

B. Rootkit

C. Adware

D. Logic Bomb

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: Computer worms are also known as Network Mobile Code, or a virus-like bit of code that can replicate itself over a network, infecting adjacent computers. A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.
A notable example is the SQL Slammer computer worm that spread globally in ten minutes on January 25, 2003. I myself came to work that day as a software tester and found all my SQL servers infected and actively trying to infect other computers on the test network. A patch had been released a year prior by Microsoft and if systems were not patched and exposed to a 376 byte UDP packet from an infected host then system would become compromised. Ordinarily, infected computers are not to be trusted and must be rebuilt from scratch but the vulnerability could be mitigated by replacing a single vulnerable dll called sqlsort.dll. Replacing that with the patched version completely disabled the worm which really illustrates to us the importance of actively patching our systems against such network mobile code.
The following answers are incorrect:
- Rootkit: Sorry, this isn't correct because a rootkit isn't ordinarily classified as network mobile code like a worm is. This isn't to say that a rootkit couldn't be included in a worm, just that a rootkit isn't usually classified like a worm. A rootkit is a stealthy type of software, typically malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer. The term rootkit is a concatenation of "root" (the traditional name of the privileged account on Unix operating systems) and the word "kit" (which refers to the software components that implement the tool). The term "rootkit" has negative connotations through its association with malware.

- Adware: Incorrect answer. Sorry but adware isn't usually classified as a worm. Adware, or advertising-supported software, is any software package which automatically renders advertisements in order to generate revenue for its author. The advertisements may be in the user interface of the software or on a screen presented to the user during the installation process. The functions may be designed to analyze which Internet sites the user visits and to present advertising pertinent to the types of goods or services featured there. The term is sometimes used to refer to software that displays unwanted advertisements.
- Logic Bomb: Logic bombs like adware or rootkits could be spread by worms if they exploit the right service and gain root or admin access on a computer. The following reference(s) was used to create this question:

The CCCure CompTIA Holistic Security+ Tutorial and CBT and
http://en.wikipedia.org/wiki/Rootkit
and
http://en.wikipedia.org/wiki/Computer_worm
and
http://en.wikipedia.org/wiki/Adware

QUESTION 474
Which of the following technologies is a target of XSS or CSS (Cross-Site Scripting) attacks?

A. Web Applications
B. Intrusion Detection Systems
C. Firewalls
D. DNS Servers

Correct Answer: A
Explanation

Explanation/Reference:
Explanation: XSS or Cross-Site Scripting is a threat to web applications where malicious code is placed on a website that attacks the use using their existing authenticated session status. Cross-Site Scripting attacks are a type of injection problem, in which malicious scripts are injected into the otherwise benign and trusted web sites. Cross-site scripting (XSS) attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user in the output it generates without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by your browser and used with that site. These scripts can even rewrite the content of the HTML page.

Mitigation:

Configure your IPS - Intrusion Prevention System to detect and suppress this traffic. Input Validation on the web application to normalize inputted data. Set web apps to bind session cookies to the IP Address of the legitimate user and only permit that IP Address to use that cookie.

See the XSS (Cross Site Scripting) Prevention Cheat Sheet See the Abridged XSS Prevention Cheat Sheet
See the DOM based XSS Prevention Cheat Sheet
See the OWASP Development Guide article on Phishing.
See the OWASP Development Guide article on Data Validation.

The following answers are incorrect:

Intrusion Detection Systems: Sorry. IDS Systems aren't usually the target of XSS attacks but a properly-configured IDS/IPS can "detect and report on malicious string and suppress the TCP connection in an attempt to mitigate the threat.

Firewalls: Sorry. Firewalls aren't usually the target of XSS attacks. DNS Servers: Same as above, DNS Servers aren't usually targeted in XSS attacks but they play a key role in the domain name resolution in the XSS attack process. The following reference(s) was used to create this question:

CCCure Holistic Security+ CBT and Curriculum
and
https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29